iControl Edge
Installation and Setup Guide

Miranda iControl

Part Number: M867-0602-103

2 February 2012

Copyright Notice

Copyright © 2006 - 2012 Miranda Technologies Inc. All rights reserved.

ATTENTION: Please read the following terms and conditions carefully. By using iControl documentation, you agree to the following terms and conditions:

Miranda Technologies Inc. hereby grants permission and license to owners of iControl to use their product manuals for their own internal business use. Manuals for Miranda Technologies Inc. products may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose unless specifically authorized in writing by Miranda Technologies Inc.

A Miranda Technologies Inc. manual may have been revised to reflect changes made to the product during its manufacturing life. Thus, different versions of a manual may exist for any given product. Care should be taken to ensure that one obtains the proper manual version for a specific product serial number.

Information in this document is subject to change without notice and does not represent a commitment on the part of Miranda Technologies Inc.

Warranty Policies

Warranty information is available in the Support section of the Miranda Web site (http://www.miranda.com).

Title	iControl Edge Installation and Setup Guide
Part Number	M867-0602-103
Revision	2 February 2012 10:44 am

toc

Table of Contents

1 Introduction to iControl Edge 1

Overview 1
- Operational Overview 2
- User Interface 2

Reference Material 3

2 System Requirements 7

Hardware Requirements 7
- iControl Edge Clients 7

Software Requirements 7
- Running Java in Windows2000 Compatibility Mode 8

Installation and Network Requirements 11
- Network Capacity 11
- Network Clients 11
- Security 11
- Network Configuration 11

3 Installation and Setup 17

Key Concepts 17

A Troubleshooting 119

Verifying Device Connectivity 119
- Troubleshooting Chart 120

B Installing PuTTY 121

Installing PuTTY 121
Establishing an SSH Connection with an Application Server 122
Ending a PuTTY Session 123

C Using WinSCP 125

Installing WinSCP 125
Logging on to an Application Server from WinSCP 129

Contact Us! 133

1 Introduction to iControl Edge

iControl Edge enables television service providers to cost-effectively monitor hundreds of television signals spread across multiple remote locations, using remotely controlled set-top boxes and receiver/decoders. It consists of a suite of existing Miranda products that have been specifically packaged into an off-the-shelf monitoring solution.

Overview

An iControl Edge system is a combination of various quantities and models of Miranda iControl, EdgeVision devices (optional), Allégro (optional), and Densité products as well as third-party set-top box infrared interface units. At each remote head-end, the set-top box signals are fed into Densité control probes or to an Allégro-1 Analog encoder/server. The signals are then streamed back to the Network Operations Center's iControl Edge monitoring system. The iControl Edge system can be easily expanded to offer set-top box monitoring of up to 16 head ends from a central Network Operations Center.

Combining the flexibility of iControl Web and the advanced processing and alarm capabilities of either EdgeVision inputs or Densité probes, iControl Edge allows any television service provider to perform comprehensive monitoring by exception of all its important video and audio signals. Using LAN and WAN connectivity, iControl Edge allows complete monitoring of multiple signals across wide geographical areas.

The system can include either EdgeVision devices or Allégro encoders (or any combination of them) for streaming remote signals in the form of full-motion video and audible audio. This allows operators, from their desktop, to listen to audio programs and to view high-quality video streams featuring multiple video images, closed captioning, audio level meters and metadata.

As a multi-signal monitoring system, iControl Edge performs simultaneous verification on multiple remote, multi-format video, audio and ancillary signals from set-top boxes, while cycling through channels. The system provides signal probing on an extensive set of signal parameters, including:

- video signal loss
- video black
- video freeze
- video luma
- macroblocking (optional)
- audio silence
- audio overload

In the event of a signal fault, the system generates alarms and provides telemetry information, which is automatically logged for reports.

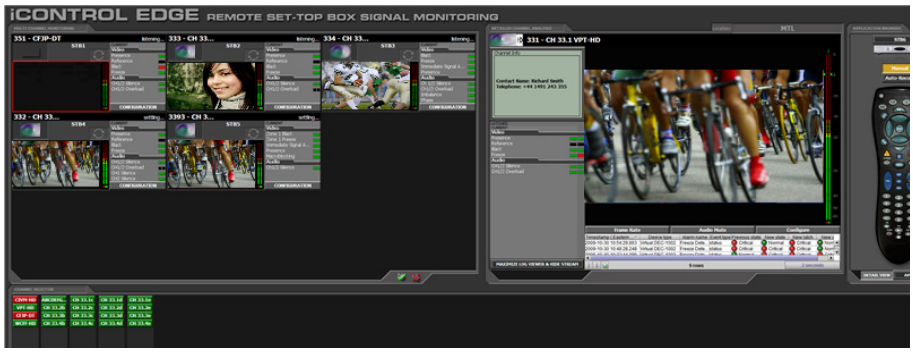
Customizable elements (e.g. station names, signal paths) are stored in spreadsheets that can be edited using the Microsoft® Excel® spreadsheet software. By adding elements to (or removing them from) a spreadsheet, you can dynamically update your monitoring system.

Operational Overview

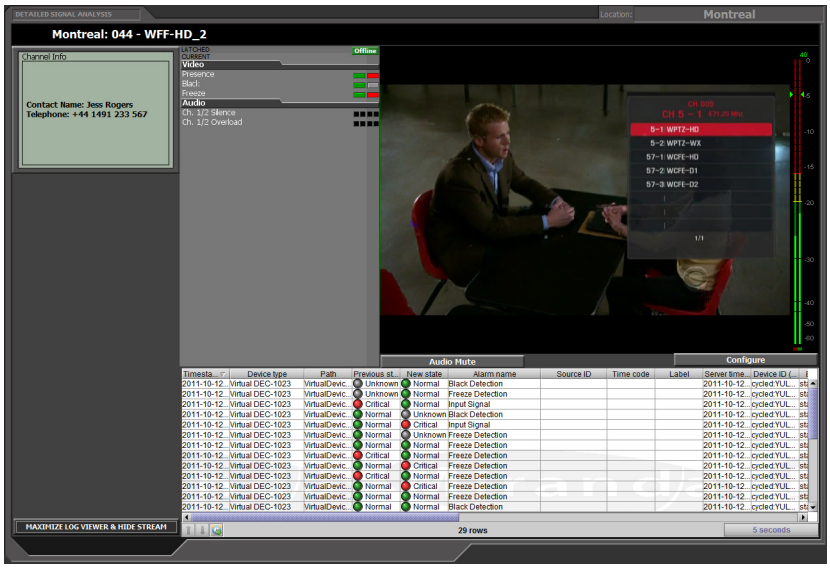
The diagram below shows the relationship between the elements of an iControl Edge system, and how they work together to provide real-time monitoring of signals.

User Interface

Once the iControl Edge system is up and running, monitoring data and live audio/video streams are automatically presented to operators within a Web page. The operator has easy access to current and historical information on every device and signal being monitored.



iControl Edge user interface (initial view)



iControl Edge user interface (Detailed Signal Analysis area)

iControl Edge user interface (Application Browser area: Application Selector, Soft Remote, and DVR Info)

iControl Edge user interface (probe configuration window, with detailed alarm panel and soft remote)

Reference Material

The table below contains a list of some of the documentation available with your iControl Edge system. Each device also ships with a set of release notes that contain important information.

Reference material

Part number	Description
M867-0602-103	iControl Edge Version 1.50 Installation and Setup Guide
M867-0700-103	iControl Edge Version 1.50 Operator's Overview
M867-0500-103	iControl Edge Version 1.50 Read Me First
M928-9900-100	EdgeVision Version 1.00 User Guide
M928-9905-101	EdgeVision Quick Start Guide
M659-9900-100	Densité CPU-ETH2 Enhanced Ethernet Controller Card Guide to Installation and Operation
M262-9900-101 **OR** M844-9900-100	Densité Housing Frame Guide to Installation and Operation **OR** Densité3 Housing Frame Guide to Installation and Operation
---	Global Caché GC-IRL IR Learner Quick Start Guide
---	Global Caché GC-100-12 Network Adapter Quick Start Guide1
M226-9900-275	iControl User's Guide (available by clicking the Documentation link on the iControl Startup Page)
M719-9900-280	Miranda Allégro-1 User Guide (available from the Allégro Startup page)

You may also need to refer to the documentation received with the set of Densité probes you ordered for your monitoring purposes.

Densité probe documentation

Video probe		**Audio probe**	
Part number	**Description**	**Part number**	**Description**
M667-9900-100	VCP-1021 Composite Video Control Probe Guide to Installation and Operation	M649-9900-104	ACP-1721 Digital Audio Control Probe Guide to Installation and Operation
--- or any of the following ---		*--- with any of the following ---*	
M761-9300-102	DEC-1002 10-Bit Composite to SDI Decoder Guide to Installation and Operation	M768-9900-101	UAP-1781 –Eight Channel Universal Audio Processor Installation and Operation Manual
M761-9400-100	DEC-1003 10-Bit Composite to SDI Decoder Guide to Installation and Operation	M768-8900-101	UAP-1783 Eight Channel Universal Audio Processor Guide to Installation and Operation
M761-9900-101	DEC-1021 12-Bit Composite to SDI Decoder Guide to Installation and Operation	M768-8200-100	AAP-1741 Four Channel Analog Audio Processor Guide to Installation and Operation
M761-9500-100	DEC-1023 12-Bit Composite to SDI Decoder Guide to Installation and Operation		

Densité probe documentation (*Continued*)

Video probe		**Audio probe**	
Part number	**Description**	**Part number**	**Description**
--- or the following probe ---		*--- with the following converter ---*	
M813-9900-110	HCP-1801HD/SD SDI Control Probe Guide to Installation and Operation	M822-9900-101	ADC-800 CAM HDV Camera HD/SD A-to-D Converter Guide to Installation and Operation
M666-9900-100	SCP-1121 Digital Video Control Probe w. Embedded Audio Guide to Installation and Operation		

Note: When referring to the documents listed above, keep in mind that the constituent products of an iControl Edge system may have features that are not supported in the context of iControl Edge.

2 System Requirements

This section lists the iControl Edge system requirements.

Hardware Requirements

iControl Edge Clients

For optimal performance, client platforms should meet the following system specifications:

iControl client platforms	Memory	Processor	Operating system
Minimum requirement for streaming video and using iCWeb	4 GB RAM	Intel Core i3 or better	Windows 7[1] or Windows XP Professional

1. On the Windows 7 platform, it is recommended to use the Java 1.6 runtime environment (update 21).

Software Requirements

You can connect to an iControl Application Server from any client PC on your network using a standard Web browser. Once you connect to a valid Application Server IP address, you can download iControl applications to your client PC. Consequently, no other application software is needed, which greatly simplifies installation and system maintenance.

Once launched, the software will continue to run on your PC, communicating with distributed network applications that may or may not reside on the Application Server where the initial connection was made.

The components of your iControl Edge system must meet the following requirements:

Device	Software version
Application Server	4.13 or later
Allégro-1 Analog (if applicable)	3.00 or later
EdgeVision (if applicable)	1.00 or later

To run any application in the iControl Edge suite, you must have the following software installed on your PC or laptop:

- a Web browser (e.g. Internet Explorer 8.0 or later, Mozilla Firefox 1.5 or later)
- Java 2 Runtime Environment (JRE) version 1.6.0_21. The installer file for the JRE (which includes Java Web Start) can be downloaded by following the **Useful Downloads** link on the iControl Startup page.

IMPORTANT: If the Java Web Start application reports errors regarding an inability to find files, it is important to clear both the Internet Explorer cache and the Java Application cache.

IMPORTANT: **Recommendation to run Java in Windows 2000 Compatibility mode**

Miranda highly recommends you switch your Java 2 JRE to Windows 2000 Compatibility mode (see "Running Java in Windows2000 Compatibility Mode", on page 8).

To modify the Configuration Spreadsheets used to define the iControl Edge monitoring layout, you will need a PC or laptop with the Microsoft® Excel spreadsheet software.

Running Java in Windows2000 Compatibility Mode

To switch your client PC's Java JRE to Windows2000 Compatibility mode:

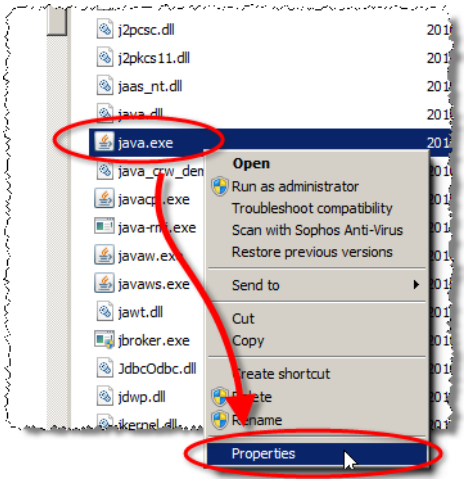
1. In Windows Explorer, navigate to the location of the following Java `*.exe` files:
   - `java.exe`
   - `javacpl.exe`
   - `javaw.exe`
   - `javaws.exe`

   Typically, you would find these files in a location such as the following:

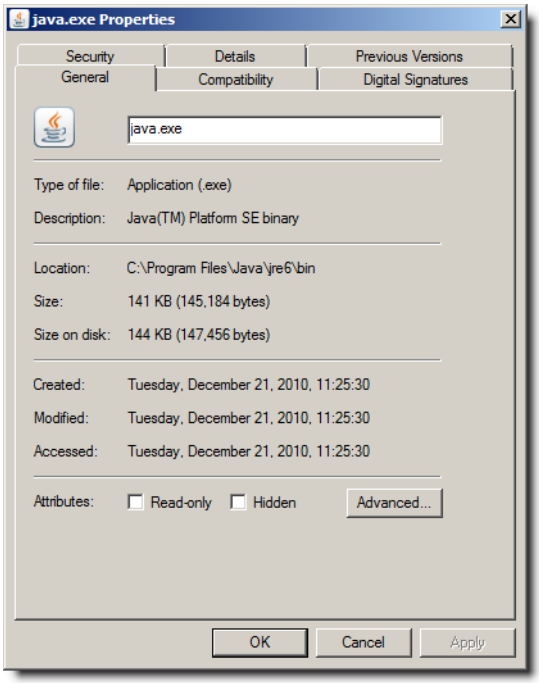
   `C:\Program Files\Java\jre6\bin`

2. Perform the following sub-steps for each of the above-mentioned files:

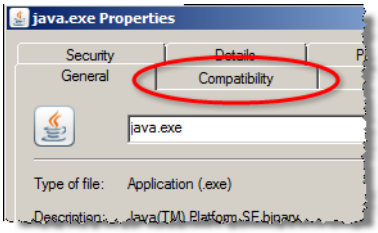
   a) Right-click the file, and then click **Properties**.



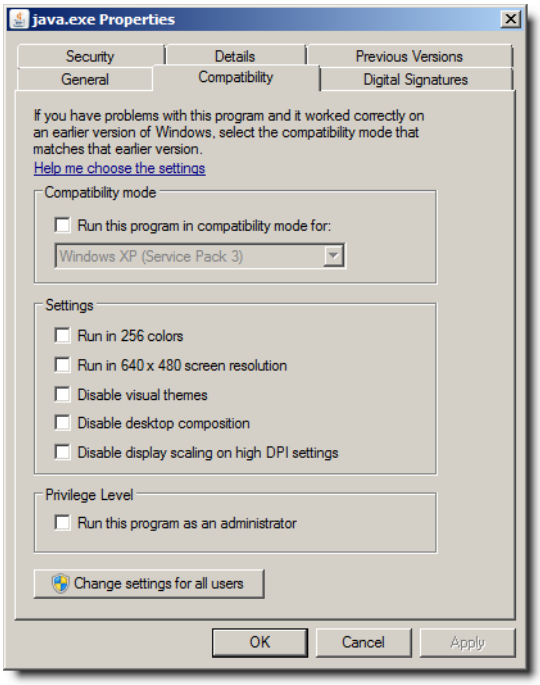
   The **Properties** window appears.



   b) Click the **Compatibility** tab.

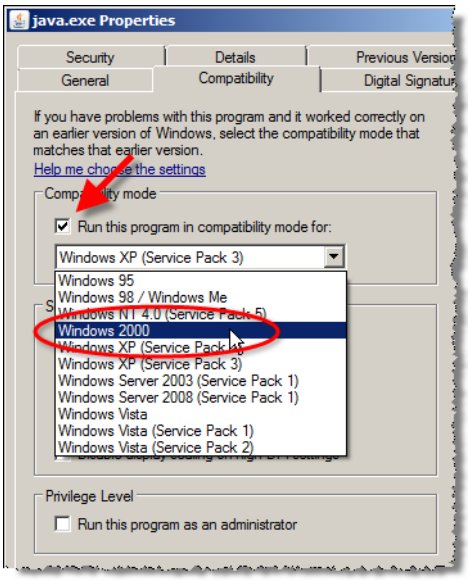


The **Compatibility** tab appears in focus.

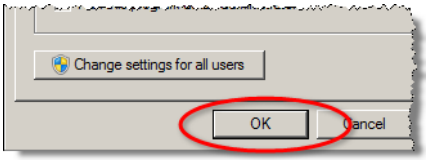

java.exe Properties
Security
Details
Previous Versions
General
Compatibility
Digital Signatures
If you have problems with this program and it worked correctly on an earlier version of Windows, select the compatibility mode that matches that earlier version.
Help me choose the settings
Compatibility mode
Run this program in compatibility mode for:
Windows XP (Service Pack 3)
Settings
Run in 256 colors
Run in 640 x 480 screen resolution
Disable visual themes
Disable desktop composition
Disable display scaling on high DPI settings
Privilege Level
Run this program as an administrator
Change settings for all users
OK
Cancel
Apply

c) Select **Run this program in compatibility mode for**.

d) From the list, click **Windows 2000**.


java.exe Properties
Security
Details
General
Compatibility
If you have problems with this program and it worked correctly on an earlier version of Windows, select the compatibility mode that matches that earlier version.
Help me choose the settings
Run this program in compatibility mode for:
Windows XP (Service Pack 3)
Windows 95
Windows 98 / Windows Me
Windows 2000
Windows XP (Service Pack 3)
Windows Server 2003 (Service Pack 1)
Windows Server 2008 (Service Pack 1)
Windows Vista
Windows Vista (Service Pack 1)
Windows Vista (Service Pack 2)
Privilege Level
Run this program as an administrator

e) Click **OK**.



Installation and Network Requirements

Network Capacity

We recommend that you install all iControl Edge devices, as well as any associated equipment, on a dedicated LAN. The quality of service of your iControl Edge system (including streaming bit rate, frame rate, and the number of concurrent users possible) is directly related to the capacity of your network.

Network Clients

Users can access the iControl Edge Application Server using a Web browser (Microsoft Internet Explorer or Mozilla Firefox) on a client PC or laptop running Windows®. When a user logs on and launches an iControl module (e.g. iC Web), the software is automatically downloaded from the Application Server and runs on the client PC or laptop.

IMPORTANT: On the client PC or laptop, the firewall must be disabled. Only one network interface card (NIC) should be enabled. It is recommended to use a wired network connection and disable any wireless adapter.

Security

iControl Edge can be incorporated into your existing security infrastructure. A qualified system administrator should verify that the setup follows your organization's security standards.

Network Configuration

Each device in your iControl Edge system arrives pre-configured with default IP address, subnet mask, and gateway address. Instructions for changing these settings to conform to your network are provided further on in this document.

Table 2-1, below, provides an overview of the default settings. Table 2-2 can be used as a worksheet for recording your new network settings.

Table 2-1:

Device	Software version
Application Server	4.13 or later
Allégro-1 Analog (if applicable)	3.00 or later
EdgeVision (if applicable)	1.00 or later

Note: iControl Edge devices may be shipped with a sticker, usually located on the top of the enclosure, identifying the default network settings.

Table 2-2: Your network settings

Device	IP Address	Subnet Mask	Gateway
--- *SETUP 1* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 2* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 3* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 4* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 5* ---			
Application Server			
Densité frame			
GC-100 network adapter			

Table 2-2: Your network settings (*Continued*)

Device	IP Address	Subnet Mask	Gateway
Allégro-1 Analog			
--- *SETUP 6* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 7* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 8* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 9* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 10* ---			
Application Server			
EdgeVision device			
Densité frame			

Table 2-2: Your network settings (*Continued*)

Device	IP Address	Subnet Mask	Gateway
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 11* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 12* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 13* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 14* ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			
--- *SETUP 15* ---			
Application Server			
EdgeVision device			

Table 2-2: Your network settings (*Continued*)

Device	IP Address	Subnet Mask	Gateway
Densité frame			
GC-100 network adapter			
--- SETUP 16 ---			
Application Server			
EdgeVision device			
Densité frame			
GC-100 network adapter			
Allégro-1 Analog			

3 Installation and Setup

iControl Edge is a distributed system, which may entail installing hardware at more than one location. An iControl Edge Application Server is usually installed at each head end, with a number of set-tops and IR network adapters, Densité probes, and an Allégro. This section describes the physical setup of the iControl Edge hardware, as well as the configuration of network settings and other software parameters.

Summary

Task 1: Preparing to Install an iControl Edge System 18
Task 2: Installing the iControl Application Server 21
Task 3: Preparing a PC for Configuring the Application Server 22
Task 4: Configuring the Application Server 26
Task 5: Installing & Configuring EdgeVision Devices 41
Task 6: Installing & Configuring Densité Systems 54
Task 7: Installing & Configuring GC-100 Network Adapters 64
Task 8: Installing Set-Top Boxes 65
Task 9: Installing & Configuring Allégro Systems 66
Task 10: Verification & Readiness Check 77
Task 11: Managing the iControl Edge Configuration Files 78
Task 12: Uploading and Applying iControl Edge Configuration Files 108

Key Concepts

Key terminology

Channel	TV or radio service that is addressable by a channel number on a set-top box (see "Services Worksheet", on page 99).
Input	A set-top box output that is used as an input to the iControl Edge system.
DVR	A set-top box that is also a digital video recorder.

Key terminology (*Continued*)

Cycling set-top box	Within the iControl Edge system, a cycling set-top box is used to automatically cycle through a pre-determined channel list (see "Services Worksheet", on page 99). Video and audio probing is usually available on this input through the use of a pair of probes (one for the video signal and one for the audio), or of a single HCP-1801 video control probe with embedded audio (in conjunction with an ADC-800 CAM converter).
Manual set-top box	Within the iControl Edge system, a manual set-top box is not used for cycling. It can be controlled via the Remote Control area of the iControl Edge Web site. If the output of this set-top box is fed to an EdgeVision (or Allégro) then it can be monitored from the **Detailed Signal Analysis** view. Streaming is usually available on this input. Probing is usually not available on this input.

Task 1: Preparing to Install an iControl Edge System

The components of an iControl Edge system are usually shipped separately. The functions of the cycling set-top box, Densité probes, and manual set-top box have been performed traditionally by separate hardware items. However, it is now possible to aggregate several of these functions into a single piece of hardware: the EdgeVision.

The advantages of using EdgeVision devices in the place of Densité probes, GC-100 network adapters, and Allégro-1 Analog systems are illustrated in, but not limited to, the following list:

- The EdgeVision device was expressly designed for use in an iControl Edge setup. As such it is optimized for the task.
- iControl Edge paired with EdgeVision devices comprise a much simpler physical setup, which takes less rack space in a smaller footprint.
- EdgeVision's cyclers provide a real video stream at up to 30 frames per second.
- EdgeVision can serve in the roles of up to three cyclers and one manual path, all in a single 1RU footprint.
- EdgeVision offers a flexibility in terms of its inputs. That is, without the need for adapters, EdgeVision accommodates HDMI, Component, and Composite inputs.
- In setups using EdgeVision, iControl Edge's overall power consumption is significantly lower than in setups not using EdgeVision.

Table 3-1 illustrates a typical setup using Densité probes, GC-100 network adapters, and Allégros, as it has been done in the past, in contrast with how the same logical setup would look using the EdgeVision device.

Note: iControl Edge continues to support the use of all of these devices.

Table 3-2 illustrates the same system-level functionality performed using EdgeVision devices instead of GC-100, Densité, and Allégro devices.

Table 3-1: Traditional hardware setup for iControl Edge (without EdgeVision)

Functionality	Network Operations Center (NOC)	Each peripheral site
Monitoring and control	1 × Application Server	1 × Application Server
Signal probing, alarming, thumbnails		n × Densité frames
Cycling set-top box		n × Global Caché GC-100 network adapters (IC-STB-CTL)
Video stream source		1 × Allégro-1 Analog system (if remote monitoring taking place at this location)

Table 3-2: Typical hardware setup for iControl Edge (using EdgeVision)

Functionality	Network Operations Center (NOC)	Each peripheral site
Monitoring and control	1 × Application Server	1 × Application Server
Signal probing and alarming		1 × EdgeVision[1]
Cycling set-top box		
Video stream source		

1. If your setup requires recording a stream's signal, you must still use an external DVR to do so.

You should inspect the shipping containers at each location to make sure that the equipment arrived undamaged, and that all materials are included. If any items are missing or damaged, contact your distributor or Miranda Technologies Inc.

Make sure the following items have been shipped with your Application Servers:

☐ Application Server

☐ Application Server hardware documentation

☐ Dell Installation DVD

☐ Rack mounting kit (rails, screws and washers)

☐ Power cord

If applicable, make sure the following items have been shipped with your EdgeVision units:

☐ EdgeVision unit

☐ Printed user documentation (Quick Start Guide)

☐ Audio/Video connector cables

☐ Ground lug

☐ Power cord

☐ Infrared cables

☐ Four rubber pads (when used as a table-top device)

☐ AC secure wire clips

If applicable, make sure the following items have been shipped with your GC-100 network adapters:

☐ Global Caché GC-100 network adapters (one for each set of 6 set-top boxes to be controlled)

☐ One AC power supply unit and AC cord

☐ Six IR emitter cables

☐ Six stick-on shields

If applicable, make sure the following items have been shipped with your Densité frames:

☐ Densité housing frame with one controller card

☐ The Densité series devices you ordered

--- *Video probes* ---	--- *Audio probes* ---
VCP-1021 Composite Video Control Probe	ACP-1721 Digital Audio Control Probe
--- *or any of the following* ---	--- *with any of the following* ---
• DEC-1002 10-Bit Composite to SDI Decoder • DEC-1003 10-Bit Composite to SDI Decoder • DEC-1021 12-Bit Composite to SDI Decoder • DEC-1023 12-Bit Composite to SDI Decoder	• UAP-1781 Eight-Channel Universal Audio Processor • UAP-1783 Eight-Channel Universal Audio Processor • AAP-1741 Four-Channel Analog Audio Processor
--- *or the following probe* ---	--- *with the following converter* ---
HCP-1801HD/SD SDI Control Probe	ADC-800 CAM HDV Camera HD/SD A-to-D Converter

☐ One ADC-800 CAM HDV camera HD/SD A-to-D converter, for each HCP-1801 module you ordered

☐ Blank rear panels (for empty slots)

☐ One AC power supply unit and AC cord

☐ A second power supply and AC cord (optional)

If applicable, make sure the following items have been shipped with your Allégro systems:

☐ Allégro unit

☐ Rack mounting kit (rails, screws and washers)

☐ AC power cord

Once the hardware components are all in place, each device must be configured to work on a common TCP/IP network. Other operational parameters, such as which alarm conditions are to be monitored, should also be configured.

Note: Densité devices ship with some pre-configured alarm settings that must be changed for proper operation of your iControl Edge system (see "Configuring the Probing Features", on page 59). Before making any such changes, please refer to the documentation specific to each device (see "Reference Material", on page 3).

You will need a PC or laptop that can connect to certain iControl Edge devices using a crossover Ethernet cable or via a network switch. The PC or laptop will need to have its network settings temporarily changed to ones that are compatible with the device.

Task 2: Installing the iControl Application Server

Miranda's Application Server is the hardware at the heart of the iControl Edge system, providing control, monitoring, logging and interface services. The Application Server is a compact 1 RU server that interfaces to other iControl devices over TCP/IP. A user can connect to the Application Server via TCP/IP from any desktop or portable computer.

Notes

- As of the release of iControl version 4.00, all Application Servers configured with new systems are Dell PowerEdge models R210 or R310. The older Dell PowerEdge 850/860 servers are still supported but may require hardware/firmware upgrades in order to run iControl Edge version 1.50.
- If your Application Server is a Dell PowerEdge model, install the faceplate after the server is placed in a rack. If your Application Server is an older Supermicro model, install the faceplate before the server is placed in a rack.

To install the iControl Application Server

1. Place the iControl Application Server in a standard 19in rack, using the rails, screws and washers provided. Make sure that the unit has adequate ventilation.
2. Connect power cords, and then turn the server on. The power switch is located on the front panel.
3. **[OPTIONAL]** Install the Miranda faceplate onto the front of the Application Server by sliding it onto the guide blocks on the side handles, then pushing it in until it clicks into place.

Notes

- An unexpected power disruption, such as might occur during a power failure, can damage the file system on an iControl Application Server. It is strongly recommended that all Application Servers be connected to a standby power source, such as a UPS (Uninterruptible Power Supply), as a preventive measure.
- Hardware documentation for the PowerEdge R310 is available from the Dell Web site:

  `http://support.dell.com/support/edocs/systems/peR310/`

Task 3: Preparing a PC for Configuring the Application Server

You will use a client PC to configure the new Application Server. The client PC must have network settings that will allow it to communicate with an iControl Application Server in its default state.

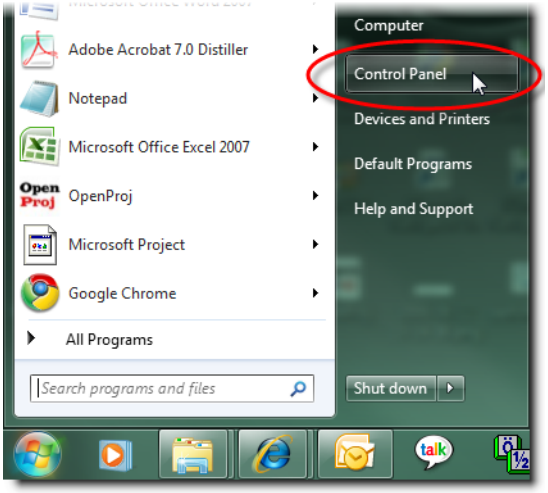
Perform one of the following procedures depending upon your client PC's operating system:

- "Configuring TCP/IP Settings of a Client PC Running Windows 7", on page 22
- "Configuring TCP/IP Settings of a Client PC Running Windows XP Professional", on page 25

Configuring TCP/IP Settings of a Client PC Running Windows 7

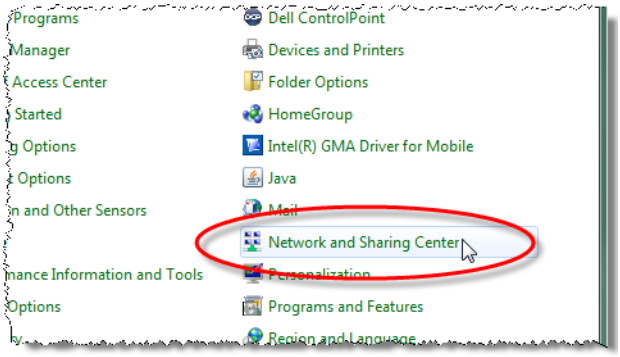
To configure TCP/IP settings of a client PC running Windows 7

1. From the Windows 7 **Start** menu, click **Control Panel**.



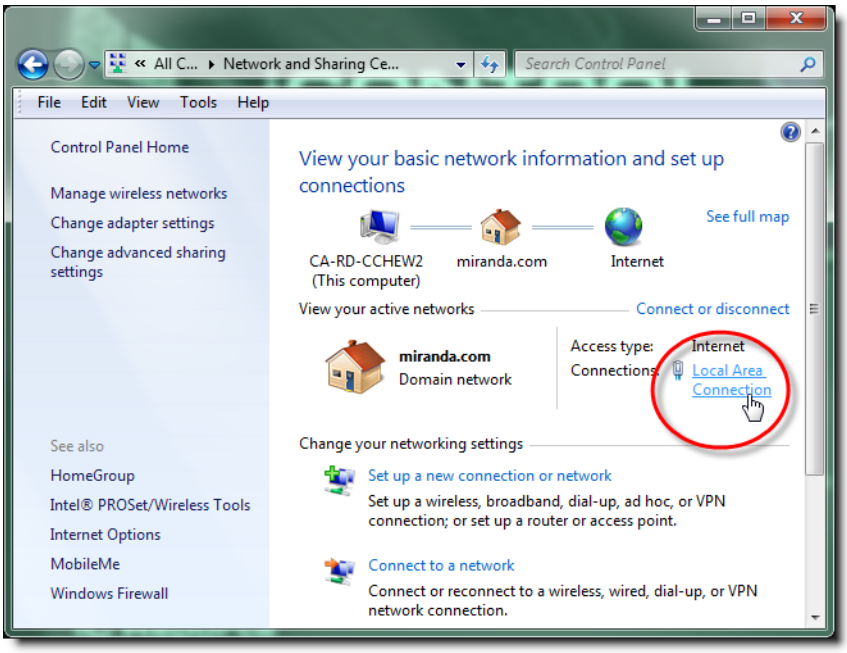
The Control Panel appears.

2. Click **Network and Sharing Center**.

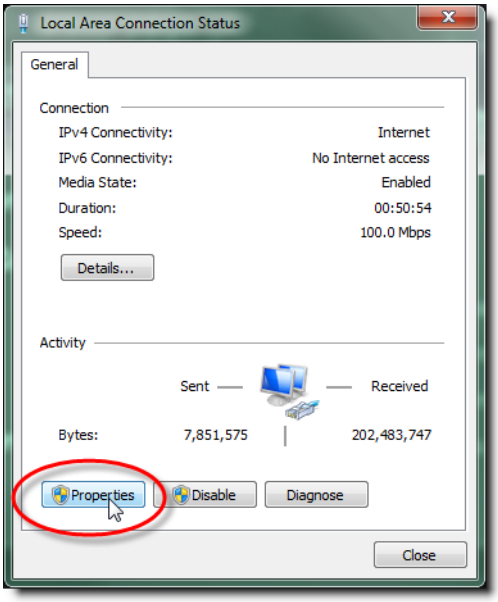


The **Network and Sharing Center** appears.

3. In the **Access type** area, click the link that corresponds to your LAN Internet connection (**Local Area Connection** in the example shown).

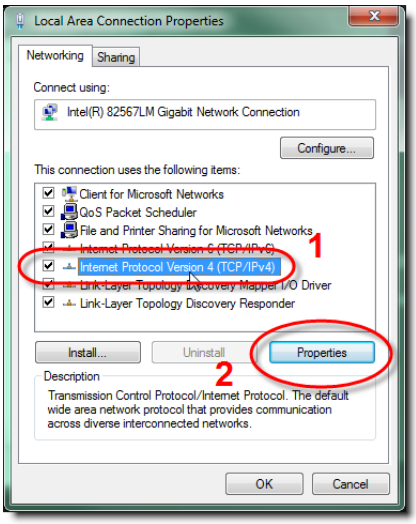

« All C... ▸ Network and Sharing Ce...
Search Control Panel
File Edit View Tools Help
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
CA-RD-CCHEW2 (This computer)
miranda.com
Internet
View your active networks
Connect or disconnect
miranda.com
Domain network
Access type: Internet
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
See also
HomeGroup
Intel® PROSet/Wireless Tools
Internet Options
MobileMe
Windows Firewall

The **Local Area Connection Status** window appears.



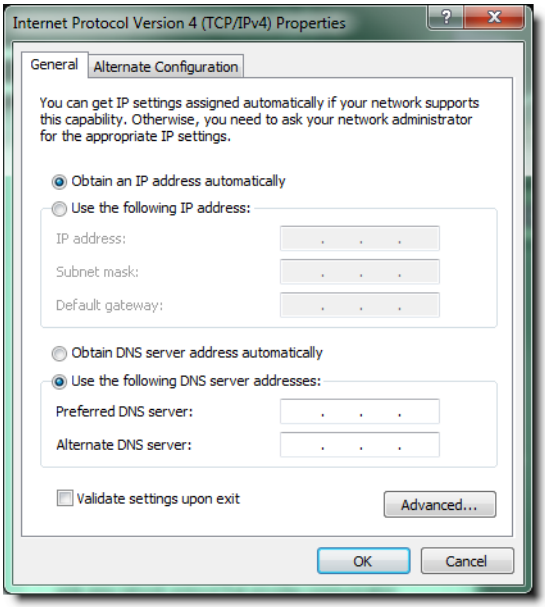
4. Click **Properties**.

   The **Local Area Connection Properties** window appears.



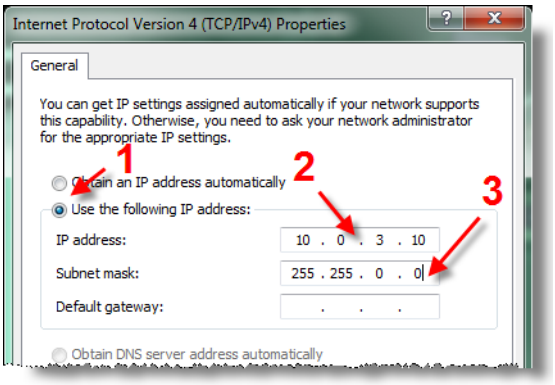
5. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

   The **Internet Protocol Version 4 (TCP/IPv4) Properties** window appears.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

6. Take note of the PC's current settings.
7. Click **Use the following IP address**.
8. The default IP address of each new iControl Application Server is `10.0.3.6`. On the client PC, type an address in the same range (e.g. `10.0.3.10`) in the **IP address** field.
9. The default subnet mask of each new iControl Application Server is `255.255.0.0`. On the client PC, type `255.255.0.0` in the **Subnet mask** field.

> **Note:** The default IP address and subnet mask settings for the Application Server are usually shown on a sticker on the top cover of its chassis.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
1
2
3
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 0 . 3 . 10
Subnet mask:
255 . 255 . 0 . 0
Default gateway:
Obtain DNS server address automatically

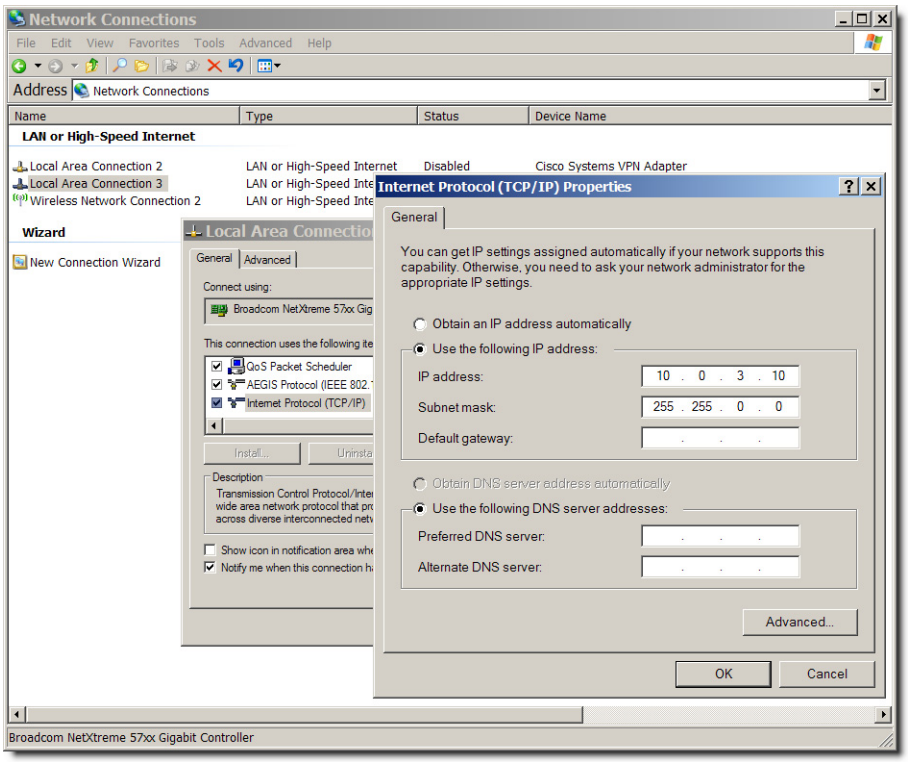
10. Click **OK** to apply these settings.
11. In the **Local Area Connection Properties** window, click **OK**.
12. Close the **Network and Sharing Center** control panel.

> **Note:** Remember to return the PC to its original network settings once you have finished configuring the iControl Application Server.

Configuring TCP/IP Settings of a Client PC Running Windows XP Professional

To configure TCP/IP settings of a client PC running Windows XP Professional

1. Open Windows Control Panel.
2. In Control Panel, click **Network Connections**.
3. Select the currently active Local Area Connection, and then right-click and click **Properties**.
4. In the **Local Area Connection Properties** window, select **Internet Protocol (TCP/IP)**, and then click **Properties**.
5. In the **Internet Protocol (TCP/IP) Properties** window, click **Use the following IP address**.


Network Connections
File Edit View Favorites Tools Advanced Help
Address Network Connections
Name Type Status Device Name
LAN or High-Speed Internet
Local Area Connection 2 LAN or High-Speed Internet Disabled Cisco Systems VPN Adapter
Local Area Connection 3
Wireless Network Connection 2
Wizard
New Connection Wizard
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 3 . 10
Subnet mask: 255 . 255 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
Broadcom NetXtreme 57xx Gigabit Controller

Configuring TCP/IP settings on a PC running Windows XP.

6. Take note of the PC's current settings.
7. The default IP address of each new iControl Application Server is `10.0.3.6`. On the client PC, type an address in the same range (e.g. `10.0.3.10`) in the **IP address** field.
8. The default subnet mask of each new iControl Application Server is `255.255.0.0`. On the client PC, type `255.255.0.0` in the **Subnet mask** field.

> **Note:** The default IP address and subnet mask settings for the Application Server are usually shown on a sticker on the top cover of its chassis.

9. Click **OK** to apply these settings.
10. In the **Local Area Connection Properties** window, click **OK**.
11. Close the **Network Connections** control panel.

> **Note:** Remember to return the PC to its original network settings once you have finished configuring the iControl Application Server.

Task 4: Configuring the Application Server

A user can connect to the Application Server via TCP/IP from any convenient desktop or portable computer. Before you can begin operations, you must configure the Application Server and make it available on your local network. The following is one possible workflow for configuring your Application Server:

Sample workflow: Configuring the Application Server

1.	Connect to the Application Server from a client PC or laptop (see page 27).
2.	Ensure that the client PC or laptop has the correct version of the Java Runtime Environment installed (see "Installing Java", on page 30).
3.	Log on to the Application Server's Webmin utility (see page 30).
4.	Configure the Application Server's network settings (see "Configuring the Network", on page 32).
5.	Apply your changes and perform a readiness check (see "Restarting the System and Verifying the Configuration", on page 39).

Connecting to the Application Server

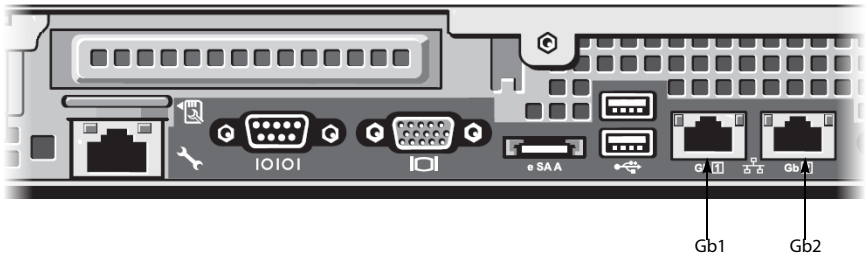
IMPORTANT: Ethernet Port Labels on the PowerEdge R210 and R310

If your Application Server is a Dell PowerEdge R210 or R310, please read the section regarding Ethernet port labels (see page 29).

To connect to the Application Server

1. Using a crossover Ethernet cable, connect the client PC to the **eth0** port on the new Application Server.

Connection between client PC and Application Server



Rear view of Application Server, showing logical ports eth0 and eth1 (physical ports Gb1 and Gb2, respectively)

Note: The default IP address and subnet mask settings for the Application Server when shipped from the factory are shown on a sticker on the top cover of the chassis above the front-panel power switch. The factory default is `10.0.3.6`.

2. Open a browser window on the client PC or laptop.
3. In the address bar, type `10.0.3.6`.

Note: The default IP address and subnet mask settings for the Application Server are shown on a sticker on the top cover of the chassis.

4. The iControl Startup Page appears.

Ethernet Port Labeling on the R210 and R310 Application Servers

The physical Ethernet ports on the backs of the Dell PowerEdge R210 and R310 are labeled as **Gb1** and **Gb2**. The physical (cabling) port called **Gb1** corresponds to logical (Webmin) port **eth0**. Likewise, the physical port called **Gb2** corresponds to logical port **eth1**. Throughout this document, when speaking of cabling and physical ports, the physical port numbers will match the logical port numbers, which is true for all types of Application Servers except the R200, R210, and R310. In the case of the R200, R210, and R310, you must map according to the table below. For example, if a procedure instructs you to connect a cable to an Application Server's **eth0** port, you must connect the cable to the R210's physical port labeled **Gb1**.

Ethernet Port Mapping on the R200, R210, and R310 Application Servers

Physical Label on R200, R210, R310	Logical (Webmin) Name
Gb1	eth0
Gb2	eth1

Navigating to the Network Configuration Page

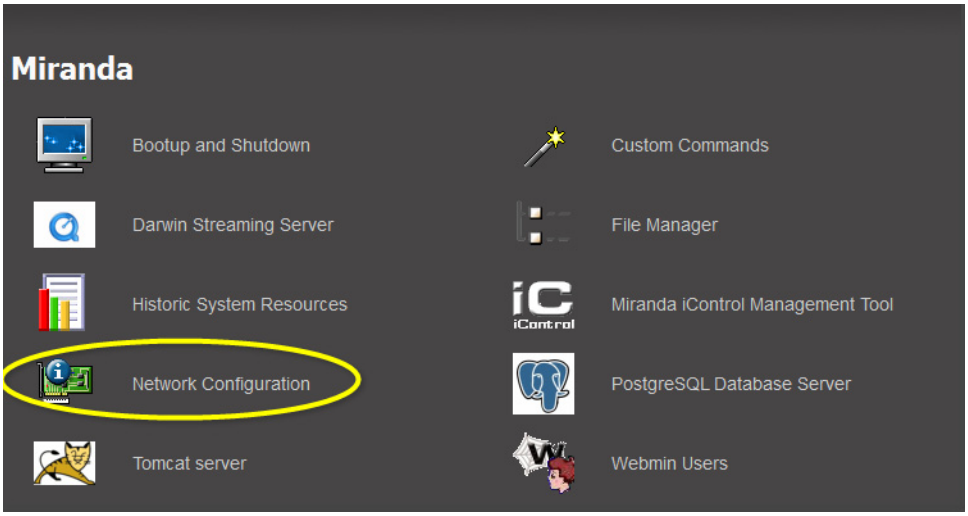
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

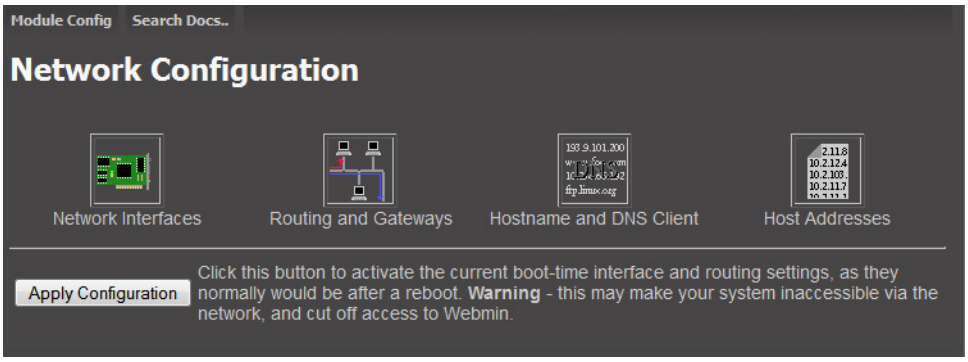
- You you have opened iControl (see "Connecting to the Application Server", on page 27).
- You are logged on to iControl Webmin (see page 30).

To navigate to the Network Configuration page

- On the Webmin page, click **Network Configuration**.



The Network Configuration page appears.


Module Config
Search Docs..
Network Configuration
Network Interfaces
Routing and Gateways
Hostname and DNS Client
Host Addresses
Apply Configuration
Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. Warning - this may make your system inaccessible via the network, and cut off access to Webmin.

Installing Java

In the course of using iControl Edge, certain software modules (e.g. iC Web) may be downloaded from the Application Server to your client PC or laptop. To run any of these iControl applications, you must have the Java 2 Runtime Environment (JRE) installed on your PC or laptop. The installer is available from the Application Server itself.

To install the Java 2 Runtime Environment on your PC or laptop

1. Click **Useful downloads** on the iControl Startup page.
2. Click **JRE for Windows**. When prompted, save the installer file (the file name should be similar to `jre-1_5_07-windows-i586-p.exe`).
3. Open the installer file.

   The installation process takes several seconds.

   Once completed, a confirmation message appears.

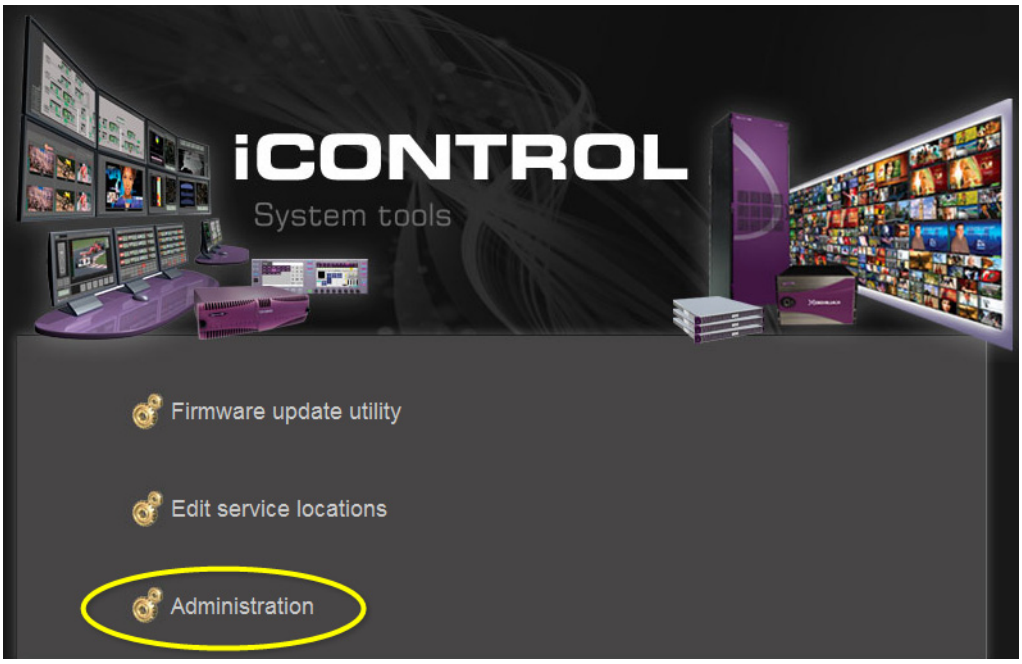
Logging on to Webmin

Webmin is the Application Server's built-in Web management utility. Logging on to Webmin is the starting point for accomplishing many tasks, including configuring the Application Server.

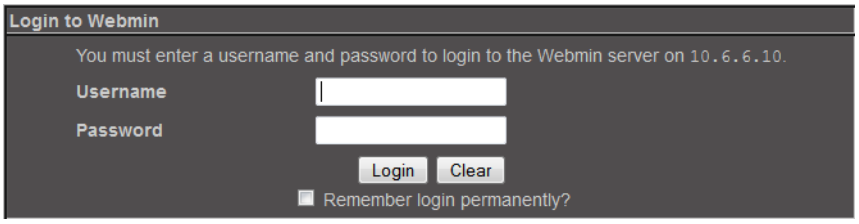
To log on to the Webmin utility

1. Click **System Tools** on the iControl Startup page.

   The System Tools page appears.
2. Click **Administration**.



The Login to Webmin page appears.



3. Type your user name and password.

   By default, these are:

   - Username: `miranda`
   - Password: `icontrol`

4. Click **Login**.

   The iControl Webmin page appears.

Configuring the Network

When configuring your network you must configure host addresses, DNS client, Gateway, and network interfaces in the proper sequence.

To configure the network

1. Specify the DNS settings to be used by your Application Server (see "Specifying DNS Client Settings", on page 33).
2. Configure your host addresses (see "Configuring Host Addresses", on page 34).
3. Specify a network gateway to be used by your Application Server (see "Specifying a Network Gateway", on page 35).
4. Configure the Ethernet interface (see "Configuring the Ethernet Interface", on page 37).
5. Add any EdgeVision devices you intend to use to the Application Server Lookup Locations list in iC Web.
6. Restart the system and verify the configuration (see "Restarting the System and Verifying the Configuration", on page 39).

Specifying DNS Client Settings

The Domain Name Service (DNS) is a type of directory service that translates host names to IP addresses and vice versa. For the most part, Application Servers and other devices on an iControl network rely on IP addresses, and so DNS is not usually needed. There are, however, circumstances where DNS is required, such as when an Application Server needs to have access to the Internet in order to display a Web page from some external source (e.g. `www.weather.com`).

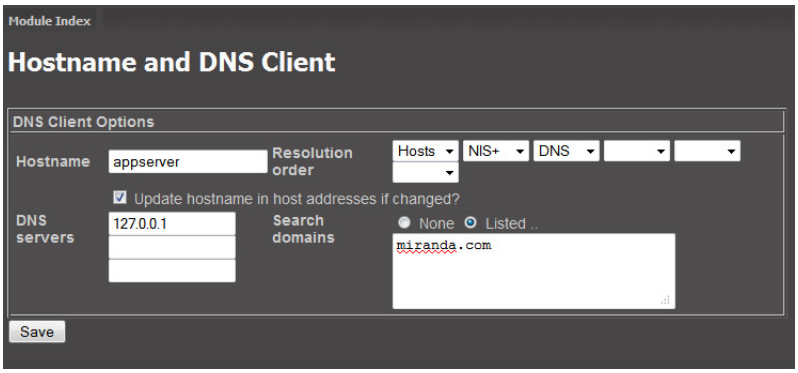
REQUIREMENT

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see page 29).

To specify the DNS settings to be used by this Application Server

1. On the Network Configuration page, click **Hostname and DNS Client**.

   The Hostname and DNS Client page appears.



2. In the **Hostname** box, type the host name by which you would like this Application Server to be known on your network.
3. Select the **Update hostname in host addresses if changed** check box.

   Note: This function ensures the host name in the Host Addresses page is the same as the host name in the Hostname and DNS Client page.

4. Configure the other parameters as required:

Resolution Order	Do not change the values in these six boxes unless your system administrator advises otherwise.
DNS Servers	The IP address `127.0.0.1`, corresponding to `localhost`, appears by default. Do not change this address. You may type the addresses of other DNS servers in the lines below. Consult your system administrator.

(*Continued*)

Search Domains	Click **Listed**, and then type a list of all the domains where you wish to have the Application Server look for DNS services (one line per domain). You should type at least your own local domain name (e.g. `miranda.com`).

5. Click **Save**.

> **Note:** Clicking **Save** does not update the Application Server with the new configuration. To apply your changes, you still need to click **Apply Configuration** on the Network Configuration page or restart the system through Webmin (see "Restarting the System and Verifying the Configuration", on page 39).

6. Return to the Network Configuration page by clicking the Return arrow at the bottom of the Hostname and DNS Client page.

> **Note:** Do not click **Apply Configuration** on the Network Configuration page.

Configuring Host Addresses

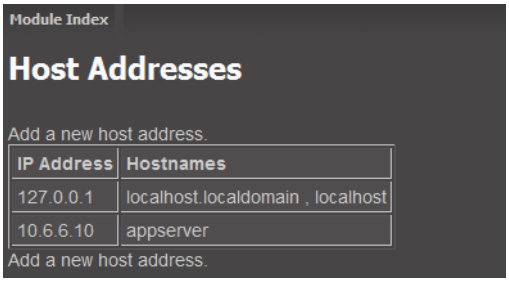
REQUIREMENT

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see page 29).

To configure host addresses

1. On the Network Configuration page, click **Host Addresses**.

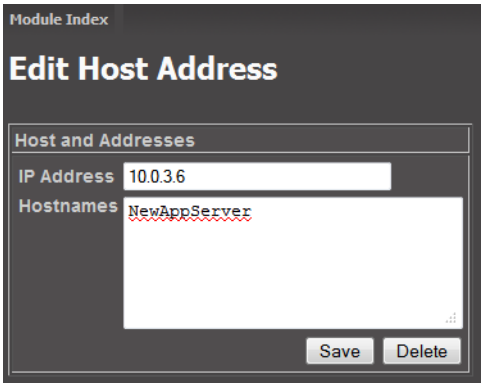
   The Host Addresses page appears. The currently defined hosts are listed, showing the IP address and host name of each.



> **Notes**
>
> - The first entry is predefined and should be left as found:
>   - IP Address: `127.0.0.1`
>   - Hostname: `localhost.localdomain, localhost`
> - The host name you defined in of should be listed here. However, you will need to assign an appropriate IP address to this Application Server.

2. Click the IP address of the Application Server (`10.0.3.6` in the example screen shown above).

   The Edit Host Address page appears.



3. In the **IP Address** box, type the IP address you would like to give to this Application Server.
4. In the **Hostnames** box, make sure the listed host name is the correct one, and then (if required) type one or more other names that will refer to this IP address.

   Note: If the host name you entered on the Host Name and DNS Client page is not accurately listed here, correct this name in the Edit Host Address page, now.

5. Click **Save**.

   The Host Addresses page reappears. The saved host names appear in the list.

   Note: Clicking **Save** does not update the Application Server with the new configuration. To apply your changes, you still need to click **Apply Configuration** on the Network Configuration page or restart the system through Webmin (see "Restarting the System and Verifying the Configuration", on page 39).

6. Return to the Network Configuration page by clicking the Return arrow at the bottom of the Host Addresses page.

   Note: Do not click **Apply Configuration** on the Network Configuration page.

Specifying a Network Gateway

In order for an Application Server to be able to send to (or receive data from) devices outside its own subnet, it must use a network gateway.

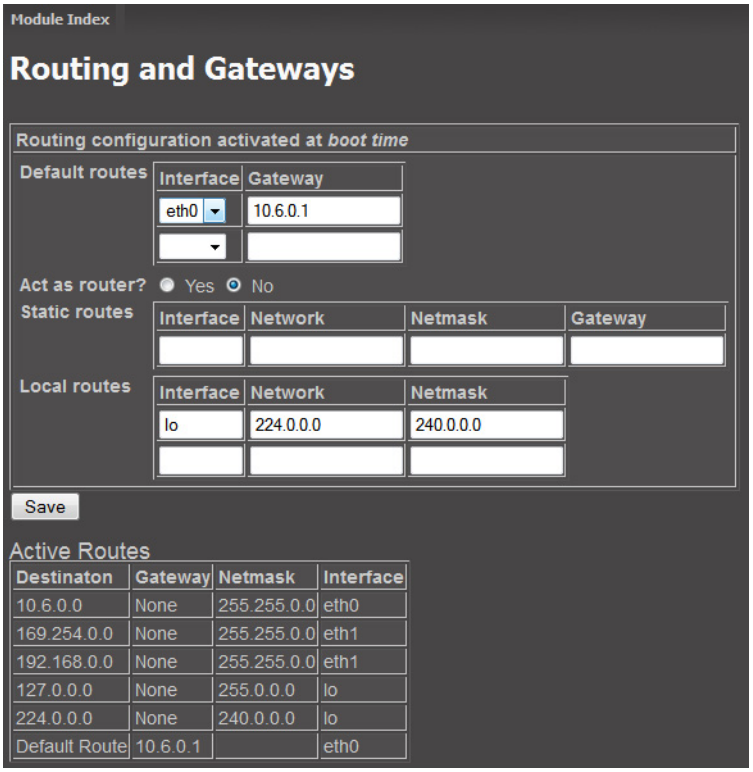
REQUIREMENT

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see page 29).

To specify a network gateway to be used by the Application Server

1. On the Network Configuration page, click **Routing and Gateways**.

   The Routing and Gateways page appears.



2. Select *eth0* from the **Interface** list in the **Default routes** area.
3. Ask your system administrator for the IP address of the network gateway that this Application Server will use, and then type this address in the **Gateway** box. If a gateway is not being used, then leave the **Gateway** box empty.
4. Click **No** beside **Act as Router**.
5. Leave the **Static routes** boxes blank.
6. In the **Local routes** boxes, do not change the value that appears for the *eth0* interface unless your system administrator advises it.
7. Click **Save**.

> **Note:** Clicking **Save** does not update the Application Server with the new configuration. To apply your changes, you still need to click **Apply Configuration** on the Network Configuration page or restart the system through Webmin (see "Restarting the System and Verifying the Configuration", on page 39).

8. Return to the Network Configuration page by clicking the Return arrow at the bottom of the Routing and Gateways page.

> **Note:** Do not click **Apply Configuration** on the Network Configuration page.

Configuring the Ethernet Interface

The Application Server is shipped with the *eth0* port turned on, in a default configuration that permits an initial connection. The default IP address setting for the Application Server is `10.0.3.6`, with subnet mask `255.255.0.0`. This section describes how to reconfigure *eth0* to meet your local network requirements.

> **Note:** You must use *eth0* as your main network interface. Client applications (e.g. iC Navigator, iC Web, etc.) must be started via the Application Server's *eth0* IP address. The other Ethernet port (*eth1*) is also configurable, but is intended for specialized use, such as connecting Miranda Densité frames and some third-party devices. New Application Servers have the *eth1* network interface disabled by default.

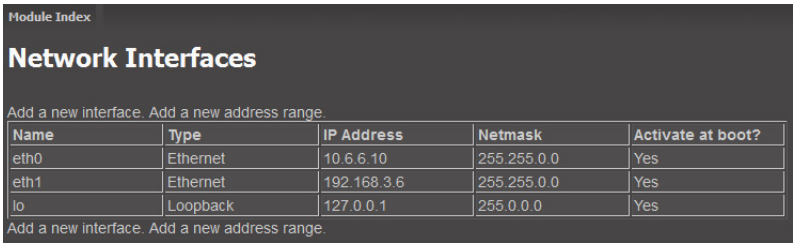
REQUIREMENT

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see page 29).

To configure the Ethernet interface

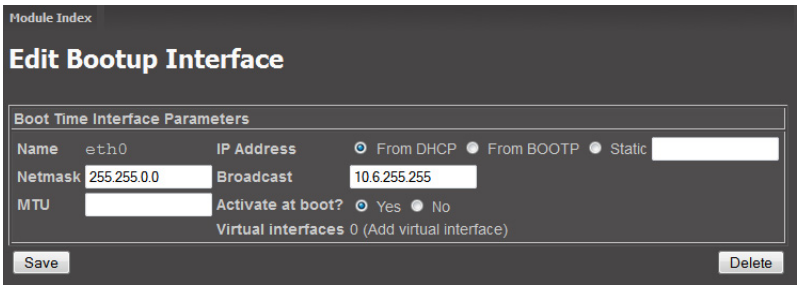
1. On the Network Configuration page, click **Network Interfaces**.

   The Network Interfaces page appears. This page shows all Ethernet interfaces currently active, and lists those that will be activated any time the system starts.


Module Index
Network Interfaces
Add a new interface. Add a new address range.
Name | Type | IP Address | Netmask | Activate at boot?
eth0 | Ethernet | 10.6.6.10 | 255.255.0.0 | Yes
eth1 | Ethernet | 192.168.3.6 | 255.255.0.0 | Yes
lo | Loopback | 127.0.0.1 | 255.0.0.0 | Yes
Add a new interface. Add a new address range.

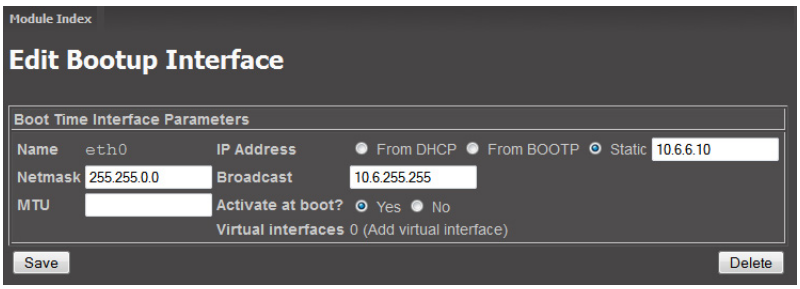
2. Click **eth0** in the **Name** column.

   The Edit Bootup Interface page appears.



> **Note:** This page shows the current settings for the *eth0* interface, which are the factory default values if you are configuring this port for the first time.

3. Click **Static**, and then type the fixed IP address you would like to use for this Application Server.



> **Notes**
>
> - Make sure you type the IP address exactly as it is on the Edit Host Address page (see step 3 of "Configuring Host Addresses", on page 34).
> - Typically the IP addresses for all devices on a LAN will begin with the same two data groups, and the remaining two will be assigned by the system administrator.

4. Type addresses in the **Netmask** and **Broadcast** boxes that correspond to your desired network configuration.

   The values you type should be based on the IP address and the desired network configuration. In the above example (`10.10.80.10`), the corresponding netmask has been configured as `255.255.255.0`, with a resulting broadcast address of `10.10.80.255`. You should always verify these values with your network administrator.

> **Note:** Leave the **MTU** box blank.

5. Click **Yes**, next to **Activate at boot**.

> **Note:** If you do not click **Yes**, the *eth0* interface will return to its previous configuration the next time the system restarts.

6. Click **Save**.

Notes

- Clicking **Save** does not update the Application Server with the new configuration. To apply your changes, you still need to click **Apply Configuration** on the Network Configuration page or restart the system through Webmin (see "Restarting the System and Verifying the Configuration", on page 39).
- The Application Server's *eth0* port is set to auto-negotiate, full duplex mode by default. This setting should not be changed. The network switch to which the Application Server is connected should also be set to auto-negotiate to avoid data packet loss.

Restarting the System and Verifying the Configuration

Once you have specified all the settings your Application Server needs to be able to operate on your local network, you must restart the system to apply the new configuration.

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

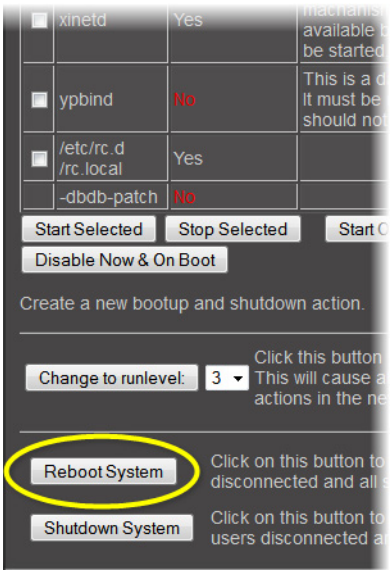
- You are logged on to iControl Webmin (see "Logging on to Webmin", on page 30).
- You have performed step 2 through step 4, inclusive, of "Configuring the Network", on page 32.

To restart the system and verify the configuration

1. On the Webmin home page, click **Bootup and Shutdown**.

The Bootup and Shutdown page appears.

2. At the bottom of the Bootup and Shutdown page, click **Reboot System**.



The Application Server restarts with the network parameters you have established.

3. Verify that the Application Server is connected to your local LAN via an Ethernet cable plugged into the *eth0* port.

4. Restore the previous network settings on the PC or laptop that were used to configure the Application Server (see "Preparing a PC for Configuring the Application Server", on page 22).
5. Verify that the Application Server is available on your network. From a workstation on the same subnet, open a browser window and type the IP address of the newly-configured Application Server. You should see the iControl Startup page.

   Alternatively, you can use the `ping` command. Open the DOS command line window on the client PC or laptop (on the **Start** menu, click **Run**), and then type the following:

   ```
   ping AAA.BBB.CCC.DDD
   ```

   where `AAA.BBB.CCC.DDD` is the Application Server's new IP address. A small window should briefly appear with a message similar to the following:

   ```
   Reply from AAA.BBB.CCC.DDD: bytes=32 time<1ms TTL=62
   ```

> **Note:** If this is a workstation that will be used to operate iControl Edge, make sure that the Java Runtime Environment is installed (see "Installing Java", on page 30).

Task 5: Installing & Configuring EdgeVision Devices

IMPORTANT: Perform this task only if you intend to use an EdgeVision **INSTEAD OF** at least one of the following:

- GC-100 network adaptor
- Densité probes
- Allégro-1 video/audio streamer

EdgeVision allows you to encode streams for up to four set-top boxes and redirect them to several computers (or third-party devices). EdgeVision can also generate multicast Transport streams, eliminating the limit to the number of devices that can receives streams.

The EdgeVision device accepts the following input types:

- Video: HDMI 1.1, Component, Composite
- Audio: Stereo Analog, S/PDIF, HDMI 1.1

The EdgeVision device is a one RU-high standalone device that you can mount in a 19in rack (for up to two channel inputs).

EdgeVision Installation Workflow

1.	Connect the EdgeVision device to the input feeds and the network or the PC that you will use to configure it (see "Connecting the Cables to the EdgeVision Device", on page 42).
2.	Update the EdgeVision software, if required (see page 43).
3.	Launch EdgeVision Admin (see page 44).
4.	Define your network parameters (see page 46).
5.	Submit the IP addresses of all your EdgeVision devices to the iControl Lookup Locations lists (see page 48)

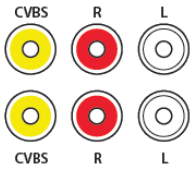
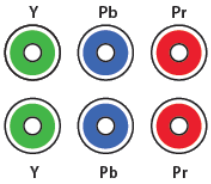
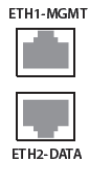
EdgeVision Installation Workflow (*Continued*)

6.	View status and configure options (see page 50.
7.	Using the EdgeVision Configurator, configure how the feeds connect to the inputs and define the Streaming parameters (including to which interface (MGMT or DATA) the streams are to be sent). You can also select which alarms to use to monitor the feed and what triggers them (see "Launching EdgeVision Configurator", on page 53).
8.	Access EdgeVision Player to monitor up to four feeds from the EdgeVision device (see the *EdgeVision User Guide*).

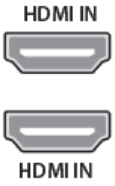
Connecting the Cables to the EdgeVision Device

The following cables can be attached to the EdgeVision device.

Connector cables and plugs

Cable	Connector Type	Input Plug	Standard/Optional
	Three-prong C-13 power cord		Standard
	CVBS cable Right/Left audio cables		Standard (3m)
	RCA		Standard (2m)
	Infrared		Standard (2m including the adhesive adaptor)
	RJ-45		Not supplied

Connector cables and plugs (*Continued*)

Cable	Connector Type	Input Plug	Standard/Optional
	SDI Connector		Not supplied
	HDMI		Optional (2m)
	S/PDIF		Optional (3m)

Updating the Software

You can update the EdgeVision device's software using the EdgeVision home page. The software updates the device's operating system. The current version of the EdgeVision device appears in Firmware major/minor fields in the **EdgeVision Admin** page (see "Viewing the Status and Configuring the Options", on page 50).

When you update the software, only the software is changed. Any configuration changes you made to the Network parameters using **EdgeVision Admin** are NOT lost when the software is updated. If a software update is interrupted, you should reboot the device and restart the software update.

To ensure that you have the latest software on your device, please contact Miranda Technical Support.

> **Note:** To perform the update, you must use the IP address for the Management port only. If you connect to the device using the IP address for the Data port, the update will be halted and the following error message will appear:
>
> `ERROR: Must use Management IP address to do upgrade`

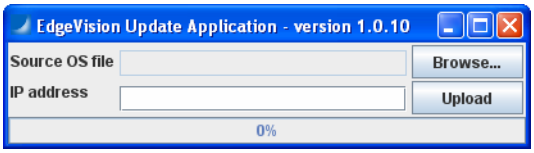
To upgrade the software on the EdgeVision device

1. Launch the EdgeVision page in a Web browser (using the IP address for the Management port).

   The EdgeVision home page appears.

2. Click the **EdgeVision link** at the bottom of the page. Accept to open the `.jnlp` file.

The **EdgeVision Update Application** appears.



> **Note:** Before the file is uploaded to the device, the updater verifies that the file is in the correct format. If the file is valid, the upload process begins. If the file is not valid, the upload is halted and the following message appears at the bottom of the dialog box:
>
> `ERROR: Input file has incorrect format`

3. Using the **Browse** button, select the file that contains the updated software (all EdgeVision software files use a `.OS` extension).

   The selected file appears in the **Source OS file** field.

4. Type the IP address for the device that you wish to update in the **IP address** field.

   The IP address for the current device appears in this field by default.

5. Click **Upload** when done.

   Once you click upload, the file is uploaded and the device reboots itself automatically, installing the software that you have selected.

6. If you are sure you are ready to continue, click **Yes**.

   Once the device reboots and the software has been updated, the EdgeVision Webpage reloads. If any sessions of EdgeVision Configurator or EdgeVision Player are running, you should shut them down and restart them.

> **Note:** While the upgrade is in progress, the EdgeVision device will stop its normal operations and reboot in *upgrade* mode, which means that it will stop doing its normal operations (e.g. no streaming, no IR control, etc.) until the upgrade is completed. When the upgrade is complete, the device reboots again in *normal* mode.

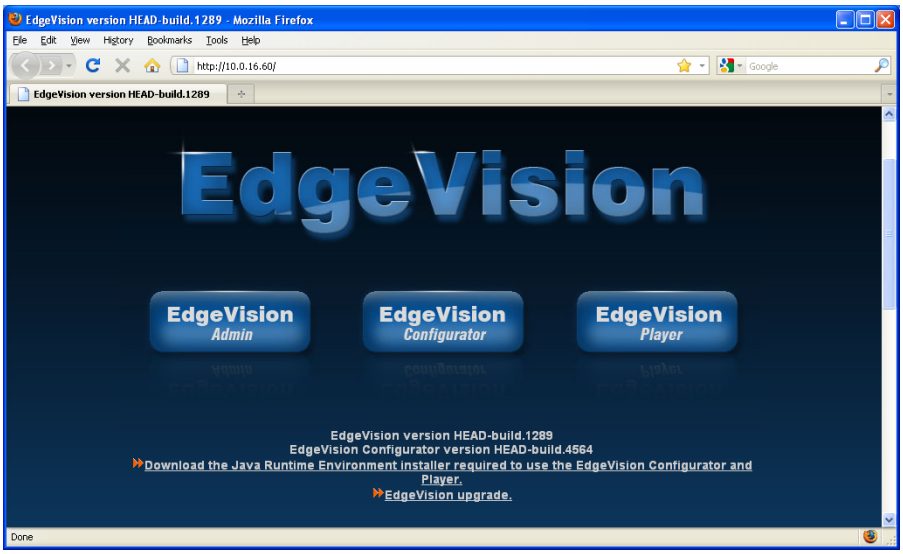
Launching EdgeVision Admin

EdgeVision Admin is a Web page that connects directly to your EdgeVision device. Not only does it display its current operational status, but it also allows you to configure its network and device properties. These device properties also appear in EdgeVision Player and EdgeVision Configurator.

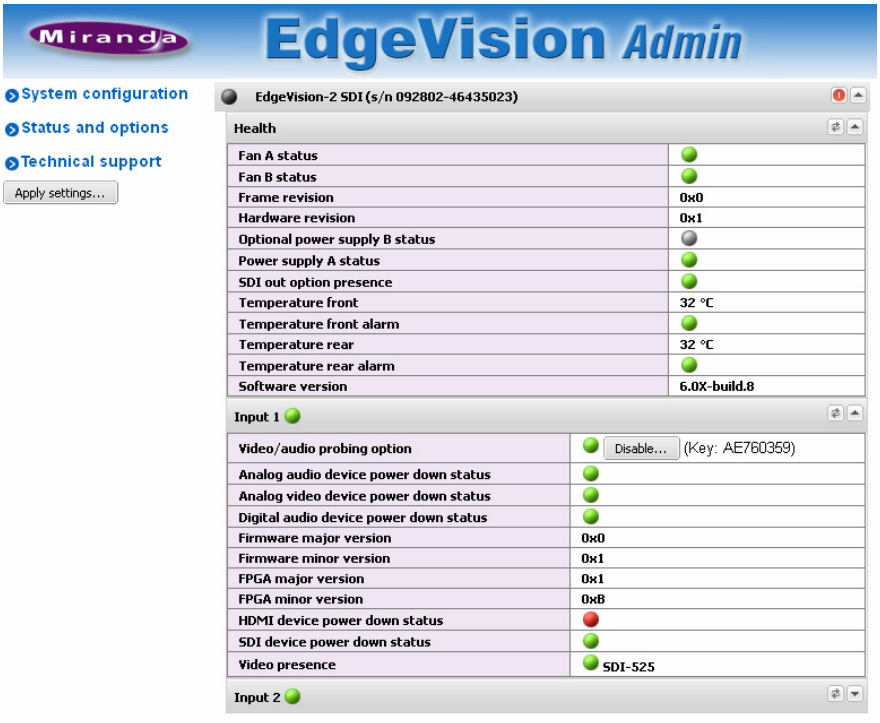
To launch EdgeVision Admin

1. Launch the EdgeVision page in a Web browser (using the device's Management IP address).

   The EdgeVision home page appears.



2. Click **EdgeVision Admin** to launch the EdgeVision Admin Web page.



LED Status Legend

LED color	Definition
Green	The feature is currently active and is operational.
Yellow	The feature is currently active, but has low importance errors.
Red	The feature is currently active but is in error.

LED Status Legend (*Continued*)

LED color	Definition
Gray	The feature is currently offline.
Black	Alarm exists, but has been disabled at the source. Some devices have the ability to deactivate certain alarms on the hardware itself, resulting in these alarms appearing black.

Defining the Network Parameters

Before you can launch EdgeVision Configurator or EdgeVision Player, you need to define the device's network parameters using the **EdgeVision Admin**. These parameters include the device's system name, IP address, and the current date and time.

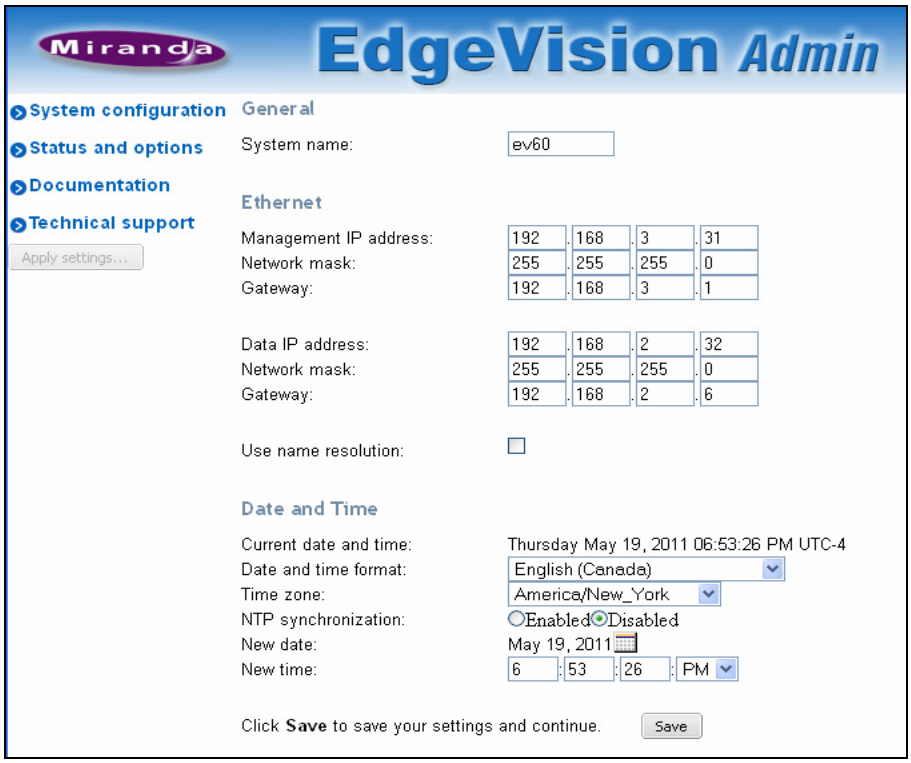
To be able to configure the network parameters for your device, you must connect to the device using the Management port IP address. You will not be able to launch EdgeVision Admin using the Data port IP address.

To define the system parameters

1. Launch the EdgeVision page in a Web browser (using the device's Management port IP address).

   The EdgeVision home page appears.

2. Click **EdgeVision Admin**.
3. Click **System Configuration**.



4. In the **System Name** field, type the name of the device as it will appear on the network, EdgeVision Configurator, and EdgeVision Player.

   You can use up to eight ASCII characters (no brackets, spaces, or tildes allowed).

5. Configure the Ethernet parameters in the **Ethernet** section as follows:

Ethernet parameters

Parameter	Definition
Management IP address	The management IP address allows the EdgeVision system to communicate with EdgeVision Configurator and EdgeVision Player , as well as being the address to forward audio/video streams generated by EdgeVision. The device remote control, configuration, and alarm collection features also use this address. **Default value**: `192.168.3.31`
Network mask	Specify the range of IP addresses that reside on the current management IP address. **Default value**: `255.255.255.0`
Gateway	Specify the IP address to use when a device from outside your network attempt to connect to the EdgeVision system via the management IP address. **Default value**: `192.168.3.1`
Data IP address	Type the IP address for the port that will stream the data to the Data Ethernet port. The data port connects the EdgeVision device to the IP network to transport IP video/MPEG data, but you can also configure it to forward of the audio/video streams generated by EdgeVision. **Default value**: `192.168.2.32`
Network mask	Specify the range of IP addresses that reside on the current Data IP address. **Default value**: `255.255.255.0`
Gateway	Specify the IP address to use when a device from outside your network attempt to connect to the EdgeVision system via the data IP address. **Default value**: `192.168.2.6`

6. Select the **Use name resolution** checkbox if you want to launch EdgeVision Player using the DATA Ethernet port.

7. Configure the synchronization parameters in the **Date and Time** section as follows:

Synchronization parameters

Parameter	Definition
Date and Time Format	Select the format in which EdgeVision displays the date and time.
Time zone	Select the time zone where the EdgeVision device resides. The time zone determines how the time is calculated.
NTP synchronization	The Network Time Protocol (NTP) is a protocol to synchronize the device clock over the data network. • If you enable this feature, the clock time is synchronized with the NTP server. Enter the IP address in the **NTP server IP address** field. • If you disable this feature, you must set the time manually in the **New Date** and **New Time** fields.
NTP server IP address	Enter the IP address for the NTP server that synchronizes the clock on this device. This field only appears if you enable the **NTP synchronization** feature.

Synchronization parameters (*Continued*)

Parameter	Definition
New date	Enter the current date for the device. This field only appears if you disable the **NTP synchronization** feature.
New time	Enter the current time for the device. This field only appears if you disable the **NTP synchronization** feature.

8. Click **Save** when done.
9. If you are ready to activate these changes on the device, click **Apply settings**.

   The device reboots itself and uses the settings you have just saved.

> **Note:** If you apply the changes and reboot the device, you may need to change the URL for the EdgeVision Admin site to the new frame IP address. You should also relaunch the EdgeVision Configurator and EdgeVision Player applications.

Adding EdgeVision Devices to the iControl Lookup Locations Lists

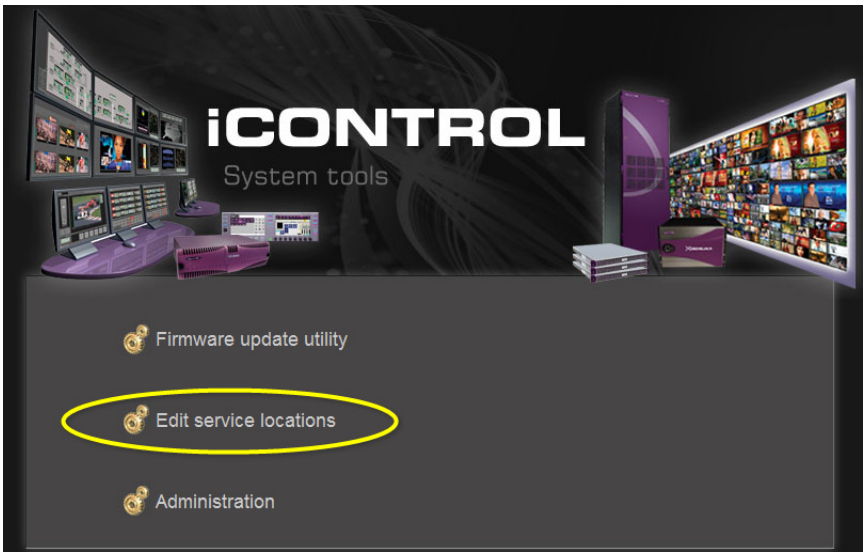
If you intend to use EdgeVision devices in your iControl Edge setup, you must first submit the IP addresses of all your EdgeVision devices to both the iControl Application Server Lookup Location list and GSM Lookup Location list, even if the EdgeVision device is on the same subnet as the Application Server.

To add EdgeVision devices to the iControl Lookup Locations lists

1. On iControl's Startup page, click **System Tools**.

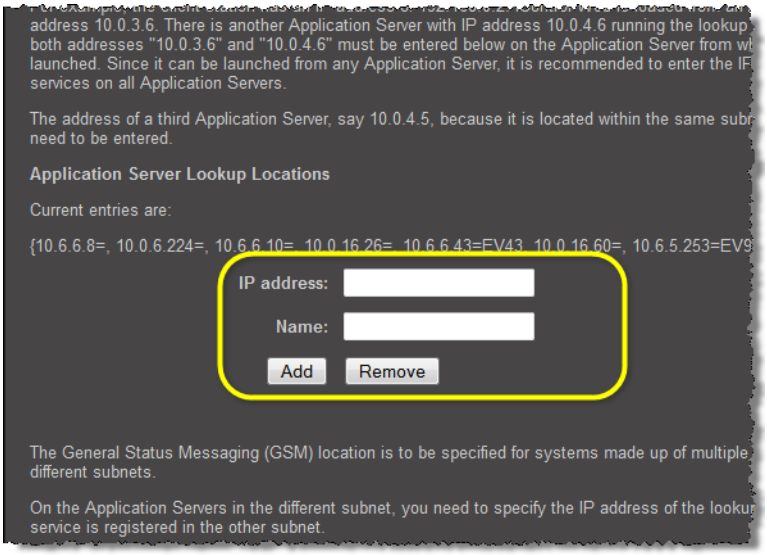
   The System tools page appears.

2. Click **Edit service locations**.



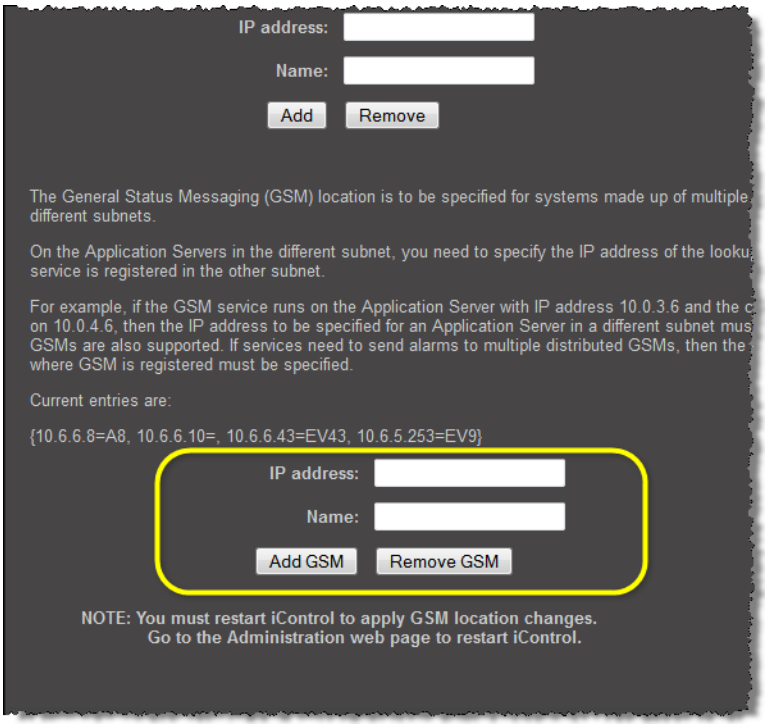
The iControl Lookup Locations page appears.

3. Enter the IP address and name for each EdgeVision device in the Application Server Lookup Locations list. Click **Add** after entering eaching IP address.


address 10.0.3.6. There is another Application Server with IP address 10.0.4.6 running the lookup
both addresses "10.0.3.6" and "10.0.4.6" must be entered below on the Application Server from wh
launched. Since it can be launched from any Application Server, it is recommended to enter the IP
services on all Application Servers.
The address of a third Application Server, say 10.0.4.5, because it is located within the same subn
need to be entered.
Application Server Lookup Locations
Current entries are:
{10.6.6.8=, 10.0.6.224=, 10.6.6.10=, 10.0.16.26=, 10.6.6.43=EV43, 10.0.16.60=, 10.6.5.253=EV9
IP address:
Name:
Add
Remove
The General Status Messaging (GSM) location is to be specified for systems made up of multiple
different subnets.
On the Application Servers in the different subnet, you need to specify the IP address of the lookup
service is registered in the other subnet.

iControl Lookup Locations page (boxes for new entries for Application Server list circled)

4. Enter the IP address and name for each EdgeVision device in the GSM Lookup Locations list. Click **Add GSM** after entering each IP address.


IP address:
Name:
Add
Remove
The General Status Messaging (GSM) location is to be specified for systems made up of multiple
different subnets.
On the Application Servers in the different subnet, you need to specify the IP address of the looku
service is registered in the other subnet.
For example, if the GSM service runs on the Application Server with IP address 10.0.3.6 and the c
on 10.0.4.6, then the IP address to be specified for an Application Server in a different subnet mus
GSMs are also supported. If services need to send alarms to multiple distributed GSMs, then the
where GSM is registered must be specified.
Current entries are:
{10.6.6.8=A8, 10.6.6.10=, 10.6.6.43=EV43, 10.6.5.253=EV9}
IP address:
Name:
Add GSM
Remove GSM
NOTE: You must restart iControl to apply GSM location changes.
Go to the Administration web page to restart iControl.

iControl Lookup Locations page (boxes for new entries for GSM locations list circled)

Viewing the Status and Configuring the Options

You can also use the **EdgeVision Admin** page to view the current status of the Inputs on the current device, as well as configure the options on the Inputs.

To view the status of the Inputs

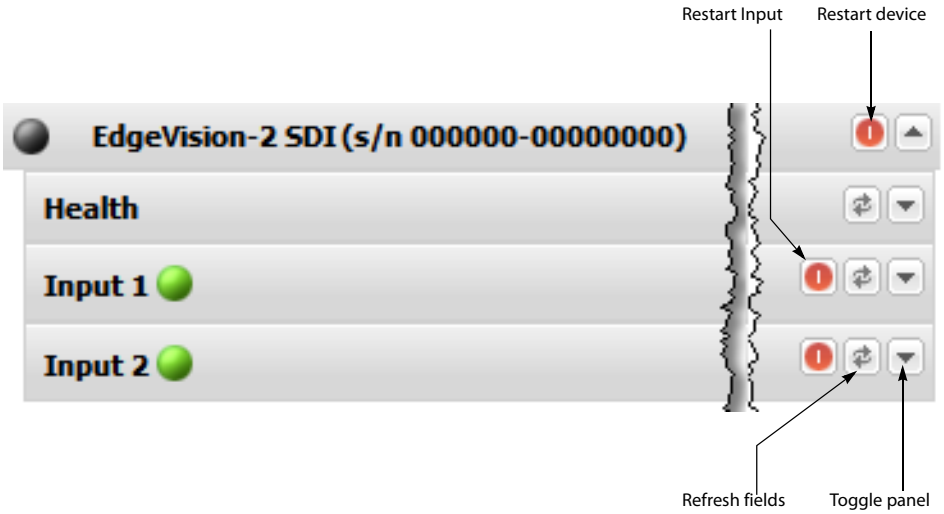
1. Using the device's IP address, access the EdgeVision page in a Web browser.

   The EdgeVision home page appears.

2. Click the **EdgeVision Admin** button.

   The **EdgeVision Admin** page appears and displays the **Status and options** panels.

Status and options panels with drop-down panels circled in red



Detail of drop-down panels on Status and options page

> **Note:** If you clicked another link and do not see the above panels, you can click the **Status and options** link to display them.

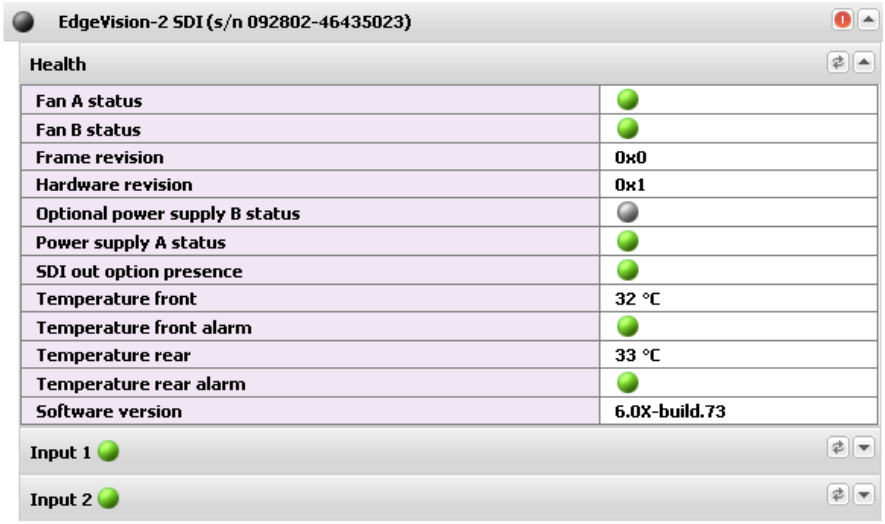
3. Click the **Status and options** link.

   A set of drop-down panels appears for the device and the Inputs that reside in it. You can hide or display these panels using the Toggle button. These panels include:

Status and Options Panels

Panel	Definition
Device	Displays the type of device that is currently active at the IP address, followed by its serial number. The device types include the following: • EdgeVision-1/EdgeVision-2/EdgeVision-4 • EdgeVision-1 SDI/EdgeVision-2 SDI/EdgeVision-4 SDI You can reboot the device by clicking **Reset EdgeVision**.
Health	Displays the status and data about the chassis. This panel appears when you open the **Device** panel.
Input #	Displays status and data about the Inputs currently in the device. There is one of these panels for each Input in the device. This panel appears when you open the **Device** panel.

4. You can view the system status by clicking the Toggle button to open the **Health** panel. The following system status fields appears:



Health status fields

Status field	Definition
Fan A/B status	Displays the current operational status of the cooling fans inside the EdgeVision device.
Frame revision	Displays the version number of the chassis that contains the hardware for the EdgeVision device.
Hardware revision	Displays the revision number for the hardware in the EdgeVision device.
Optional power supply B status	Displays the current operational status of the secondary (B) power supply.
Power supply A/B status	Displays the current operational status of the primary (A) power supply.
SDI out option presence	Indicates if the SDI out option is present on the EdgeVision device.
Temperature front/rear	Displays the current temperature in the front of the device (where the LEDs reside) and in the rear of the device (where the connectors are located).
Temperature front alarm/rear alarm	Indicates if the current temperature in the front or rear of the device has exceeded optimal limits.
Software version	Displays the current build version of EdgeVision Configurator and EdgeVision Player on this device.

5. You can view the status of an Input by opening the Input # panel. To refresh the list of status', click the Refresh button. The following input status fields appears:

Input status fields

Input status field	Definition
Analog audio device power down status	For debug purposes only.
Analog video device power down status	
Digital audio device power down status	
Firmware major version	
Firmware minor version	
FPGA major version	
FPGA minor version	
HDMI device power down status	
SDI device power down status	
Video presence	Displays the the format detected on the input (ex. SDI-525).

6. To enable the Video/audio probing option, click **Enable** next to the **Video/audio probing** option field and enter the option key provided by Miranda Technologies Inc.

Launching EdgeVision Configurator

To be able to configure the alarms and flags on your device, you must connect to the device using the Management port IP address. You will not be able to launch EdgeVision Configurator using the Data port IP address.

See also

For more information about the IP address of the Management port, see "Defining the Network Parameters", on page 46.

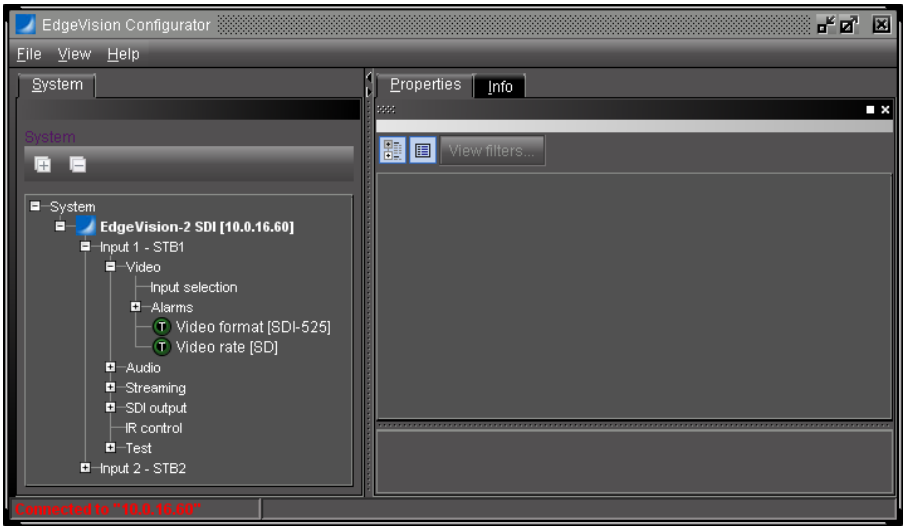
To launch EdgeVision Configurator

1. Launch the EdgeVision page in a Web browser (using the device's Management IP address).

   The EdgeVision home page appears.

2. Click **EdgeVision Configurator**.

   EdgeVision Configurator opens.



Task 6: Installing & Configuring Densité Systems

> **IMPORTANT:** Perform this task only if you are **NOT** installing an EdgeVision for the purposes of probing signals.

Densité modules housed in your Densité frames process video and audio signals from set-top boxes and relay monitoring data and alarms to the iControl Edge Application Server.

Installing Densité Frames

To install a Densité frame

1. Install the housing frame directly into a standard 19in rack using 4 standard rack-mounting screws.
2. Fit all received Densité series cards and rear panels into the frame, referring to the Densité Housing Frame Guide to Installation and Operation for detailed instructions (see "Reference Material", on page 3).
3. Make the appropriate video, audio and network connections, referring to the Densité CPU-ETH2 Enhanced Ethernet Controller Card Guide to Installation and Operation, to learn how to connect your Densité system to the network, and to the documentation included with each card (see "Reference Material", on page 3).
4. Connect the supplied AC power cord to the rear-panel AC receptacle, and secure it with the retainer clip attached to the receptacle.
5. Plug the power cord into an AC outlet to turn the unit on.

Configuring Densité Services

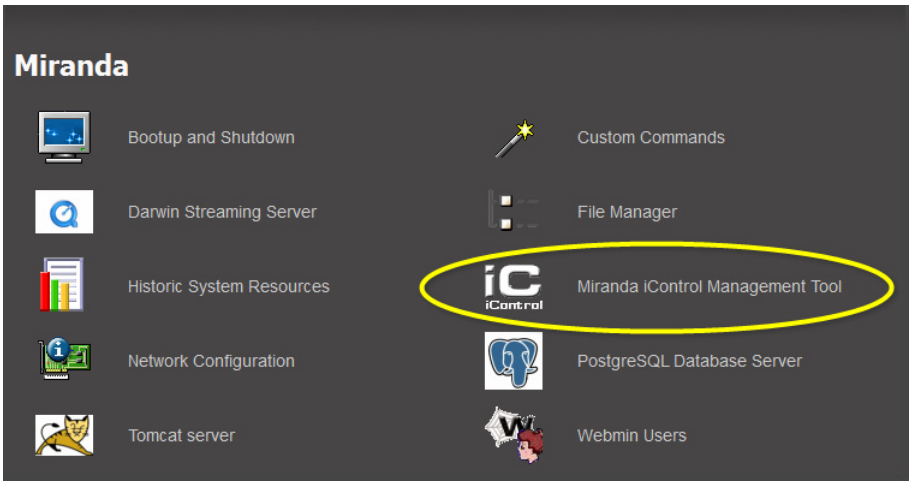
Before you can begin operations, you must configure Densité Manager and Densité Communicator services to make your Densité frames and the associated Densité modules available on your local network. Specifically, you may have to:

- enable at least one Densité Manager service on the Application Server
- access the appropriate Densité Manager control panel and add a Densité Communicator service for each Densité frame included in your system
- access your Densité card's control panels to enable thumbnails and audio level meters, and to configure video and audio alarms.

Enabling Densité Manager Services

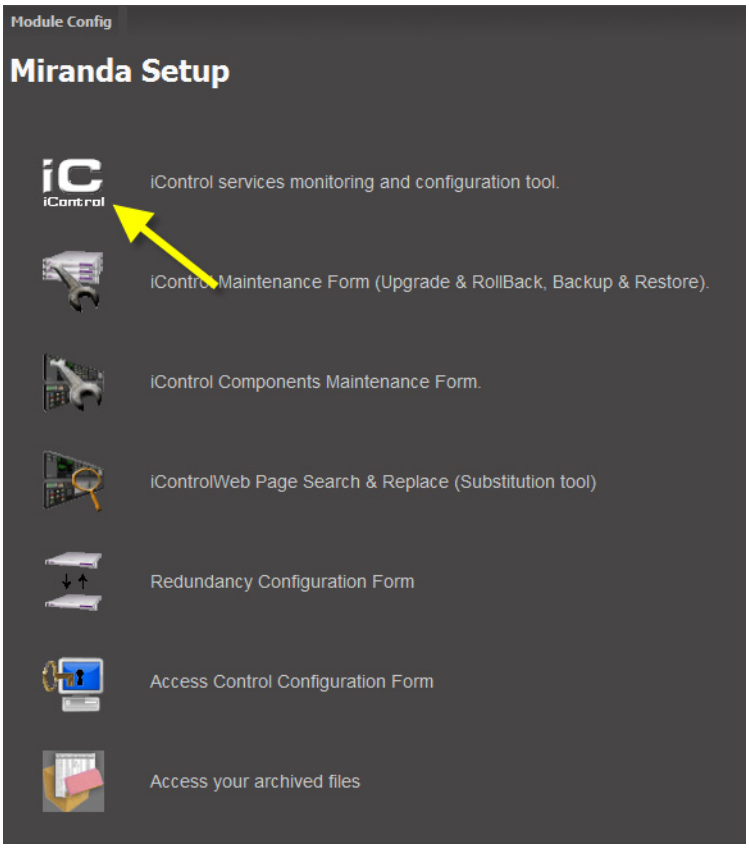
To enable a Densité Manager Service

1. Log on to Webmin (see "Logging on to Webmin", on page 30).
2. Click **Miranda iControl Management Tool**.

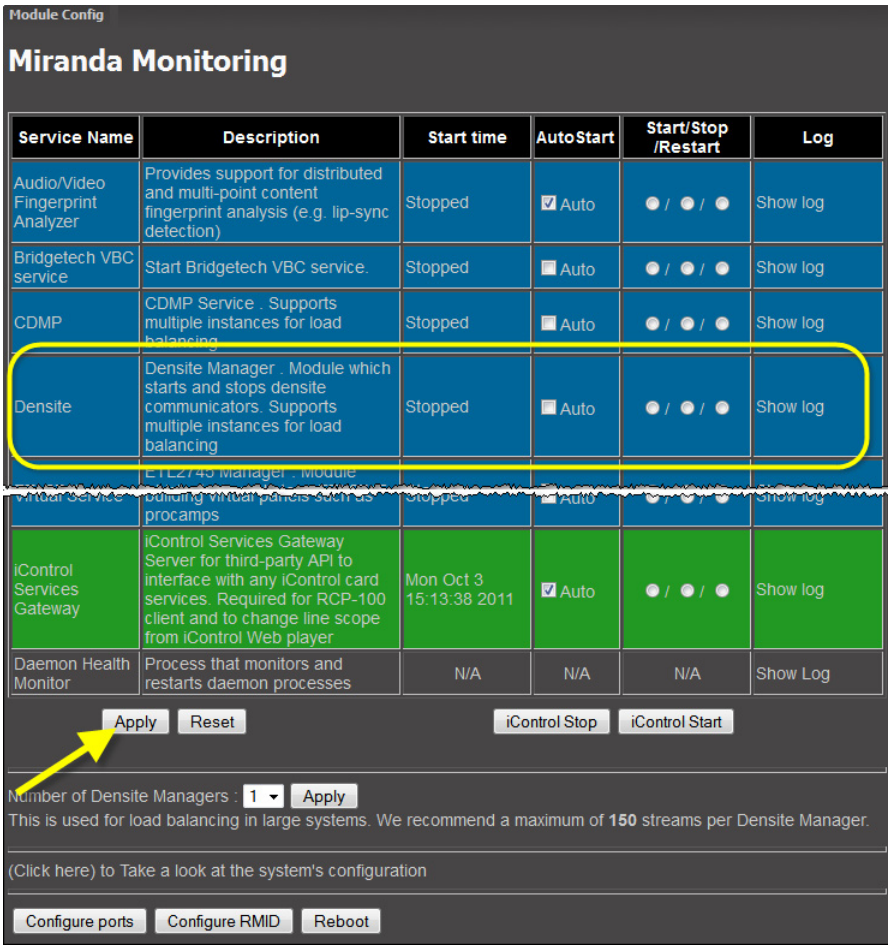


The Miranda Setup page appears.

3. Click the iControl logo next to **iControl services monitoring and configuration tool**.


Module Config
Miranda Setup
iControl services monitoring and configuration tool.
iControl Maintenance Form (Upgrade & RollBack, Backup & Restore).
iControl Components Maintenance Form.
iControlWeb Page Search & Replace (Substitution tool)
Redundancy Configuration Form
Access Control Configuration Form
Access your archived files

The Miranda Monitoring page appears.



Miranda Monitoring page (Densité Manager Service circled)

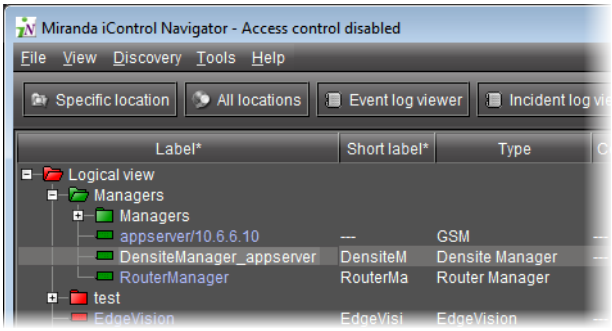
4. Find the row corresponding to the Densité Manager service.
5. In the **Start/Stop/Restart** column, select the **Auto** check box, click the **Start** option button, and then click **Apply** at the bottom of the page.

> **Note:** If you need to increase the number of Densité Managers, select the appropriate number for your purposes from the list at the bottom of the page, before clicking the Apply button next to it.

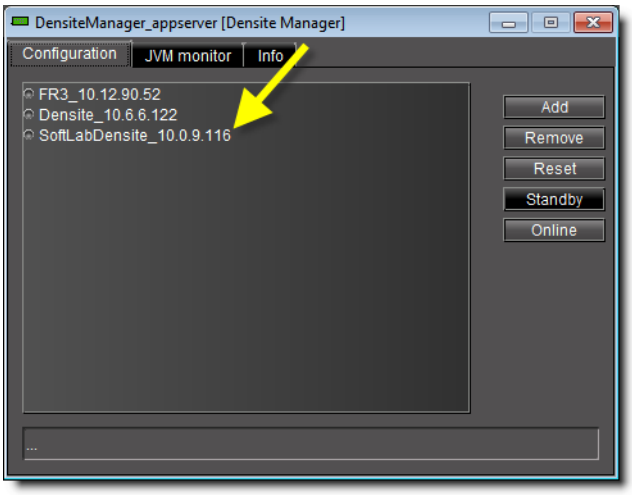
Adding Densité Communicator Services

To add a Densité Communicator service

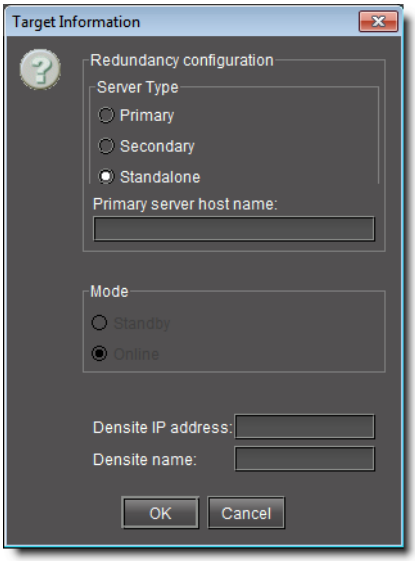
1. Open iControl Navigator.
2. Double-click DensiteManager in the logical view.



3. In the Densite Manager window, click **Add**.



4. In the **Target Information** window, type the Densité frame's IP address and a descriptive name for the new Densité Communicator service.



5. Click **OK**.

The new Densité Communicator will be started and added to the list. The Application Server will query the corresponding Densité frame, and any devices (e.g. cards) it discovers will be displayed in the iControl Navigator window.

6. Repeat this procedure until you have added Communicator services for every Densité frame in your iControl Edge configuration.

See also

For more information about Densité Communicator services (also called Densité Frame services), see the *Configuring Devices & Services* chapter in the *iControl User Guide* (see "Reference Material", on page 3).

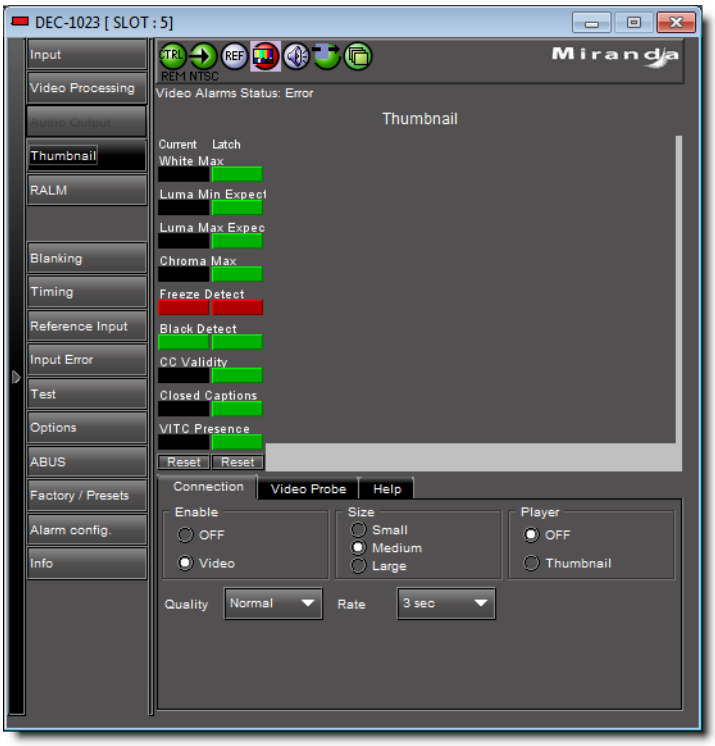
Configuring the Probing Features

For each Densité module in your iControl Edge configuration, you need to enable thumbnail streaming and/or audio level meters. You must also configure the appropriate video and audio alarms for your monitoring purposes, and disable all logging to avoid filling the system logs with irrelevant entries.

Enabling Thumbnail Streaming

To enable thumbnail streaming on a video probe

1. In iControl Navigator, select the Densité card you wish to configure.
2. On the **View** menu, click **Show control panel**, to open the card's control panel.
3. Click the control panel's **Thumbnail** tab.
4. Under **Enable**, click **Video**.
5. Under **Size**, click **Large**.
6. Select **Fast** from the **Rate** list.



Example of a control panel showing Thumbnail settings

Enabling Audio Level Meters

The procedure below is an example showing how to enable the appropriate audio level meter on HCP-1801 cards. Some steps may vary, depending on your actual card model. Refer to the documentation that shipped with the card you wish to configure (see "Reference Material", on page 3).

To enable audio level meters

1. In iControl Navigator, select the Densité card you wish to configure.
2. On the **View** menu, click **Show control panel**, to open the card's control panel.
3. Click the control panel's **RALM** tab.
4. Under **RALM remote control**, select the **AES1** check box.
5. Select **Fast** from the **Speed** list.

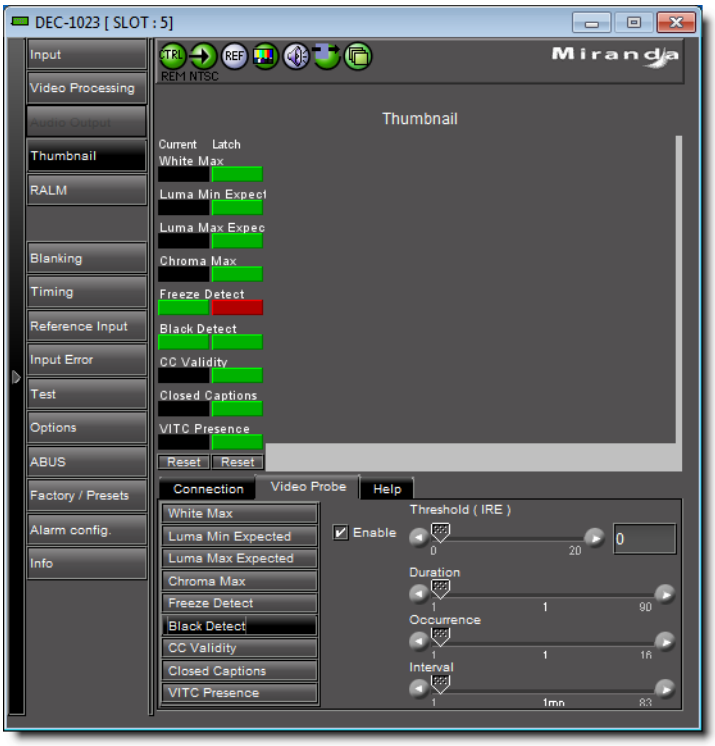
Example of a control panel showing RALM settings

Configuring Alarm Settings

To configure relevant alarms on a Densité probe

1. In iControl Navigator, select the Densité card you wish to configure.
2. On the **View** menu, click **Show control panel**, to open the card's control panel.
3. Enable and configure all relevant alarms (e.g. video black and freeze, audio silence and overload).

> **Note:** Make sure to set the alarm duration to the lowest value (typically 1 second) and the number of occurrences to 1.



Example of a control panel showing enabled video black alarm settings

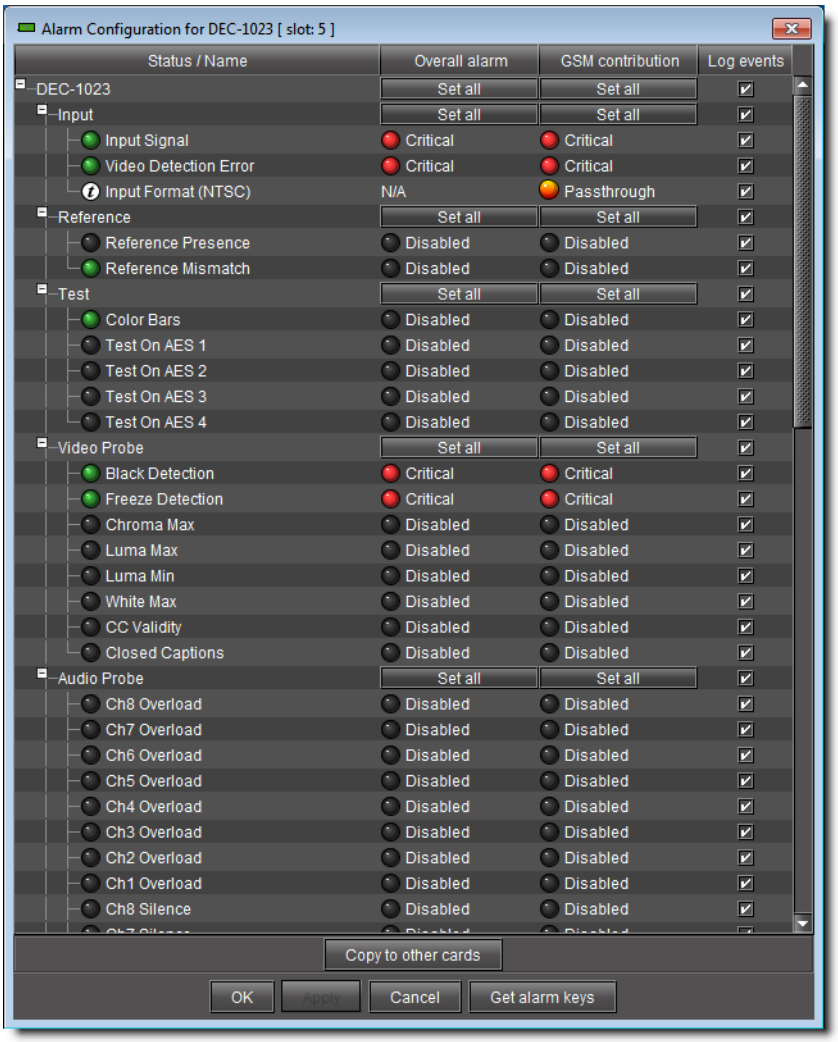
4. Click **Alarm config**.

   The **Alarm Configuration** window for this Densité probe opens.

5. In the **Log events** column, clear the first check box to disable all event logging for this probe.

   This will avoid filling the event log with irrelevant entries.

6. For each alarm you enabled for this card, set the appropriate overall and GSM contribution.



Alarm configuration example

7. Once all relevant alarms are enabled and configured for this card, click **Copy to other cards**.

   The **Copy to other cards** window appears, displaying a list of all cards of the same type.

8. For each card to which you wish to copy the current alarm configuration, select the corresponding check box.
9. Select the **All** check box at the top of the column to select all the available cards.
10. Select the **All** check box again to remove all check marks.
11. Click **Copy**.

    A successful copy is indicated for each card by the appearance of the word Succeeded in the **Transfer status** column.

12. Click **Close** to close the **Copy to other cards** window.
13. Click **Profiles** at the bottom left of the control panel.

The **Profile copy for card** window appears, with the current card identified under **Copy profile from**. All other cards of the same type are listed under **Copy profile to**.

14. For each card to which you wish to copy the current profile, select the corresponding check box in the **Select** column.
15. Select **Select All** at the top of the column to select all the available cards.

> **Note:** The copy profile operation is prohibited when a target card does not have the same firmware version as the source card. In such cases, the designation `N/A` will appear on a yellow background in the **Transfer status** column.

16. Click **Copy**.

    A successful copy is indicated for each card by the appearance of the word `Succeeded` in the **Transfer Status** column.
17. Click **Exit** to close the **Profile Copy for Card** window.
18. Close iControl Navigator.

    This will also close any control panels that were left open, and other secondary windows.

Task 7: Installing & Configuring GC-100 Network Adapters

IMPORTANT: Perform this task only if you are **NOT** installing an EdgeVision for the purposes of sending IR commands to STBs.

Install and configure your GC-100 units to make them available on your local network. You also need to configure the appropriate number of IR or Sensor connectors on each unit as IR output. Refer to the *Global Caché GC-100-12 Network Adapter Quick Start Guide* (see "Reference Material", on page 3 for details).

Configuring the GC-100 IR Service

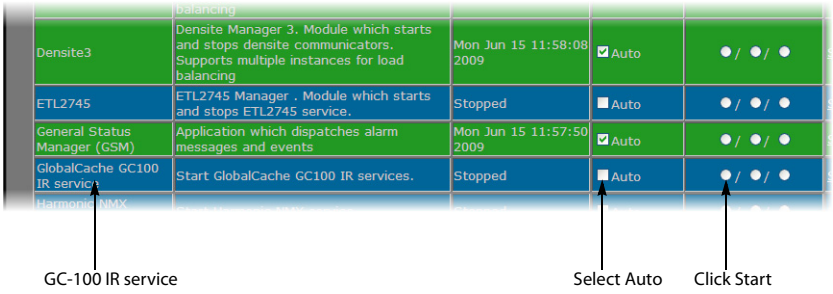
Once your GC-100 units are connected to your local network you must enable the GC-100 IR service on the Application Server.

To enable the GC-100 Service

1. Log on to Webmin (see "Logging on to Webmin", on page 30).
2. Click **Miranda iControl Management Tool**.

   The Miranda Setup page appears.
3. Click the iControl logo next to **iControl services monitoring and configuration tool**.

   The Miranda Monitoring page appears.
4. Find the row corresponding to the GC-100 IR service.



5. In the **Start/Stop/Restart** column, select the **Auto** check box, click the **Start** option button, and then click **Apply** at the bottom of the page.

Task 8: Installing Set-Top Boxes

A number of set-top boxes will typically be controlled from cycler services on the Application Server via an EdgeVision unit or GC-100 network adapters. If your system includes an Allégro streaming encoder/server (or a streaming EdgeVision), then one set-top box will be manually controlled, either from the associated remote control unit, or from the soft remote in the Application Browser area of the iControl Edge's Web site.

Connecting a GC-100 Network Adapter to a Cycling Set-Top Box

To connect a GC-100 network adapter to a cycling set-top box

- Plug one end of an IR emitter cable to an IR output on the GC-100, and position the other end against the IR receiver on the set-top box front panel.

> **Note:** You may want to shield the link between the IR emitter cable and the IR receiver on the set-top box by using protective adhesive tape (e.g. duct tape), to prevent adjacent set-top boxes from picking up IR commands that are not targeted at them.

Connecting a Set-Top Box to an HCP-1801

To connect a set-top box to an HCP-1801 video control probe with embedded audio

- If using an HCP-1801 video control probe with embedded audio, then you need to insert an ADC-800 CAM converter between the set-top box and the HCP-1801 probe (refer to the documentation that shipped with these devices).

Connecting a Set-Top Box to a Pair of Densité Probes

To connect a set-top box to a pair of Densité probes

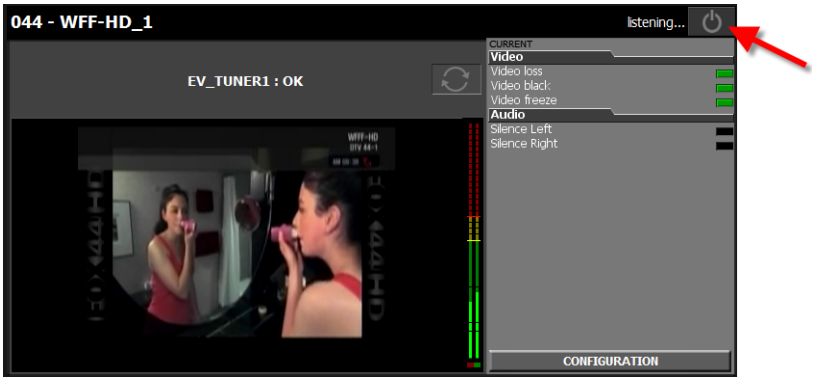
1. Using appropriate cables, connect the composite video output on your set-top box to a BNC input at the back of the appropriate video probe in your Densité frame (refer to the documentation for your specific set-top box model and Densité probe).

2. Connect an RCA cable to the appropriate audio connectors from the back of your set-top box to the back of the appropriate audio probe in your Densité frame (refer to the documentation for your specific set-top box model and Densité probe).

Power Cycling (through TCP/IP) a Set-Top Box

If your Set-Top Box is powered with an APC7900 power bar, and your spreadsheet is configured with the appropriate APC7900 information (in the *PDU* section), you will be able to remotely power-cycle your STB simply by clicking the Reboot button ( ). The Reboot button is in two locations in iControl Edge:

- Beside the player in the **Multi-Channel Monitoring** area



- Beside the STB icon in the **Application Browser** when in **Remote Control** view.

Task 9: Installing & Configuring Allégro Systems

IMPORTANT: Perform this task only if you are **NOT** installing an EdgeVision for the purposes of processing and monitoring video streams over IP.

The Allégro is the component of the iControl Edge system that provides a streaming solution for remote monitoring. The Allégro encodes and transmits video and audio streams in real time with low latency, making them available to multiple clients simultaneously via IP. It is designed for continuous, autonomous operation, and is entirely integrated into the iControl Edge environment.

The Allégro-1 Analog is a one-channel streaming encoder server with composite video input and analog stereo audio input. It allows video encoding (in aspect ratios of both 4:3 and 16:9) to resolutions that range between 80 × 64 and 640 × 480, using Miranda's proprietary MVC-1, MVC-2 and MVC-3 video codecs.

Note: Allégro is designed to work in a secure private network with a bandwidth that is proportional to the desired audio and video streaming quality as well as the number of simultaneous users. Due to performance considerations, a maximum of 16 simultaneous users can be connected to the streaming source from an Allégro.

Installing Allégro Systems

In a basic configuration, one Allégro system is installed at each site to be monitored.

To install an Allégro system

1. Install the Allégro in a standard 19in rack, using the rails, screws and washers provided. Make sure that the unit has adequate ventilation.
2. Make the appropriate video, audio and network connections.
3. Connect the supplied AC power cord to the rear-panel AC receptacle, and secure it with the retainer clip attached to the receptacle.
4. Plug the power cord into an AC outlet to turn the unit on.

Configuring Allégro systems

Before you can begin operations, you must configure each Allégro and make it available on your local network. Specifically, you may have to:

- access the Allégro
- configure network and other settings
- set up streaming relays
- apply your changes and perform a readiness check

Accessing the Allégro

The Allégro has a built-in Web-based management utility. This utility is available as soon as the system is powered up, and can be used to configure the system using a Web browser on any PC or laptop, provided the PC or laptop can reach the Allégro's IP address.

To access the Allégro system

1. Configure your Client PC or laptop with an IP address in the same range as the IP address of the Allégro (see "Preparing a PC for Configuring the Application Server", on page 22).
2. Open a Web browser and type the Allégro's default IP address (see "Network Configuration", on page 11), specifying a connection on port 8080.

   `http://10.3.0.7:8080/`

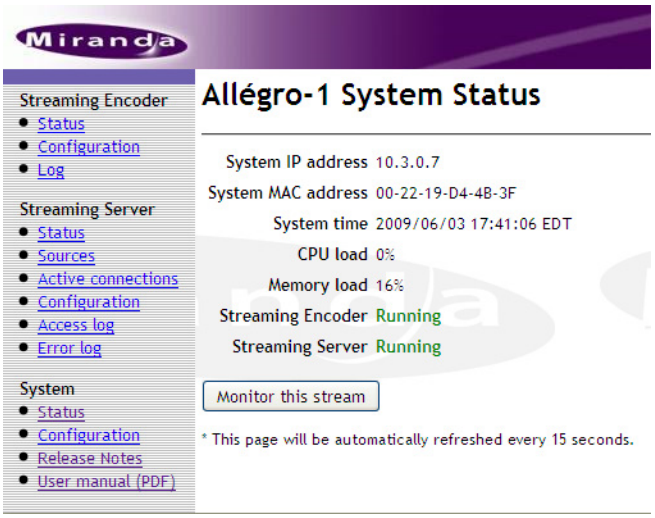
   The Allégro Startup Page appears.

Configuring the Allégro

To configure the Allégro system

1. Click **Administration page** on the Allégro Startup page.
2. When prompted, type `admin` in the **User Name** box, type `16streams` in the **Password** box, and then press **Enter**.

   The System Status page appears.



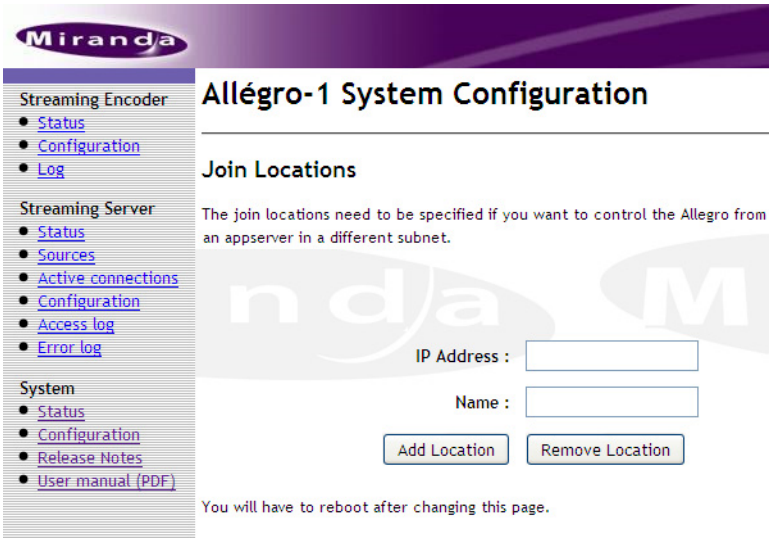
Allégro System Status page

3. Click **Configuration** under the **System** heading in the bottom part of the navigation bar.

   The System Configuration page appears.

4. Click **Edit Join Locations**.

   The Join Locations page appears.

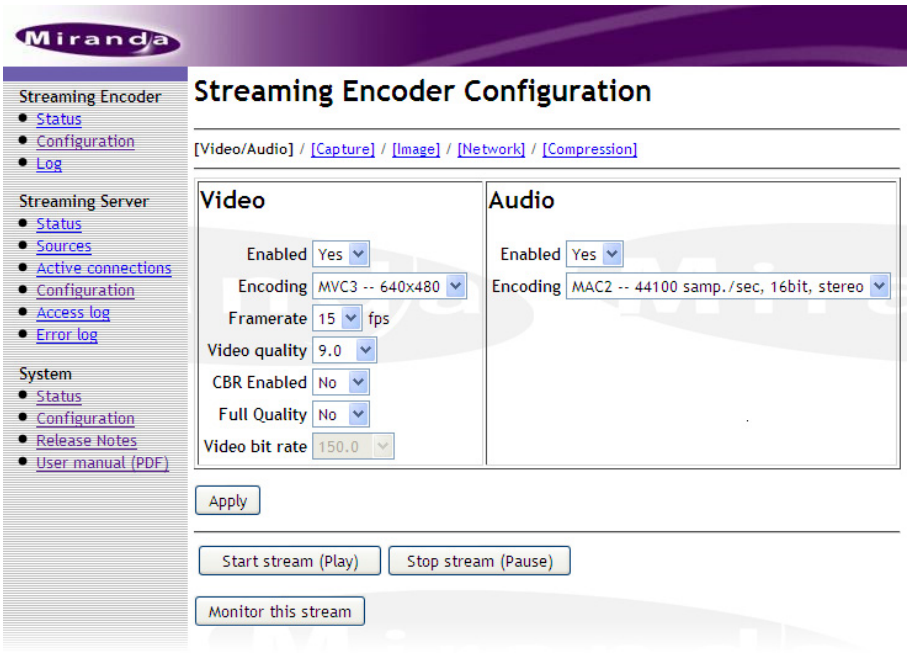


5. Type the new IP address and host name of the Application Server, and then click Add Location.
6. Click **Configuration** under the **System** heading in the navigation pane, and then click **Edit GSM Locations** in the main pane.

   The GSM Location page appears.

7. Type the new IP address and host name of the Application Server, and then click **Add GSM**.
8. Click **Configuration** under the **Streaming Encoder** heading in the left pane.

   The Streaming Encoder Configuration page appears.

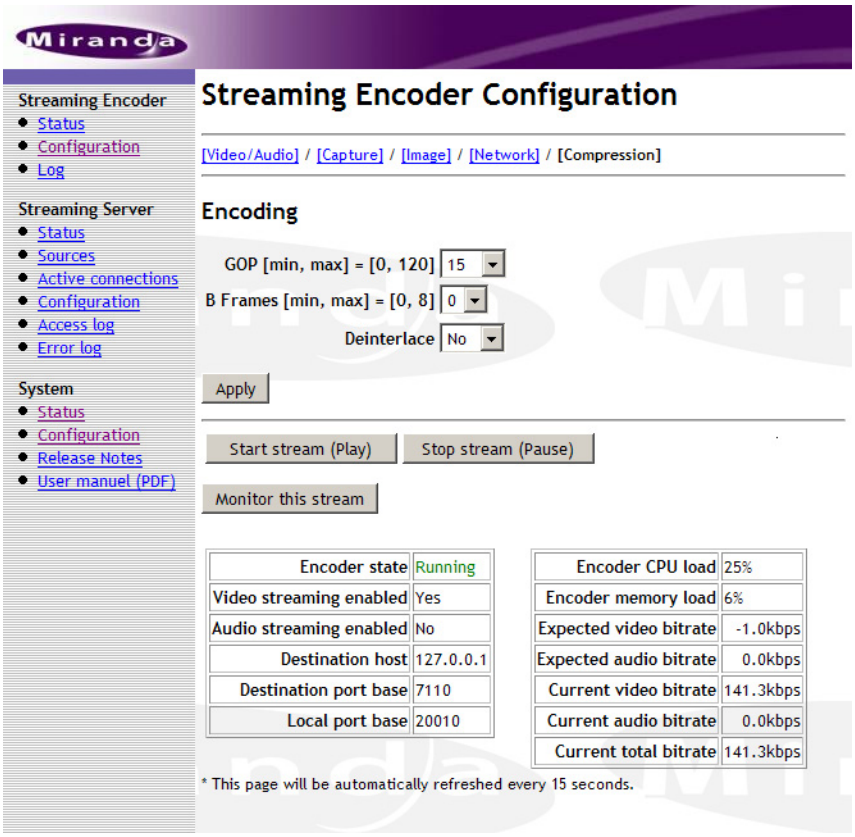


Streaming Encoder Configuration page (Video/Audio)

9. In the **Video** section, make sure **Enabled** is set to `Yes`.
10. In the **Video** section, select the encoding, frame rate, and video quality as follows:

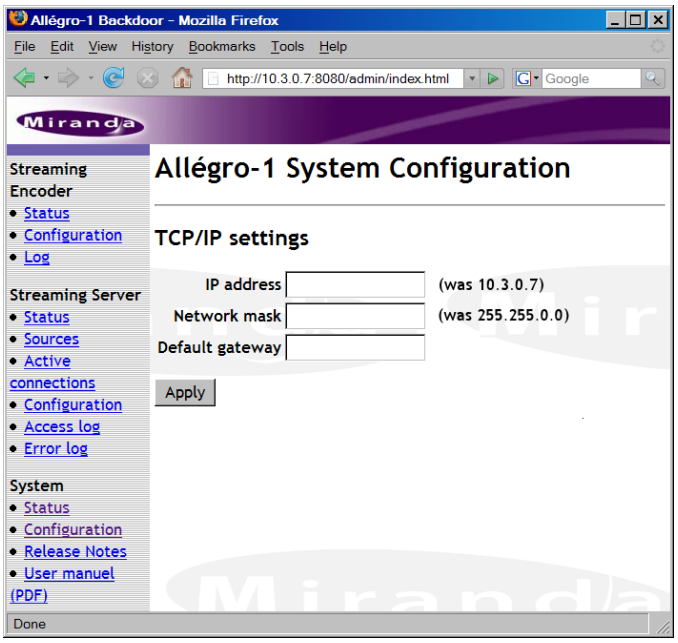
Parameter	Recommended value
Encoding	MVC3 -- 640 × 480
Frame rate	15 (or less)
Video quality	9.0

11. In the **Audio** section, make sure the **Enabled** setting is `Yes`.
12. In the **Audio** section, set **Encoding** to `MAC2-44100 samp./sec, 16 bit, stereo`.
13. Click **Apply**.
14. Click **Compression** in the navigation bar near the top of the Streaming Encoder Configuration page.



15. In the **Encoding** section, make sure the **Deinterlace** setting is No.
16. Click **Apply**.
17. Click **TCP/IP settings** in the right panel.

    The TCP/IP settings page appears.



18. Type the new IP address, network mask, and default gateway address in the corresponding boxes, and then click **Apply**.

Configuring Allégro Streaming Relays

In an iControl Edge configuration, operators typically monitor audio/video streams from several remote locations at once. Having each remote Allégro send a stream to multiple operators over a WAN can result in performance problems. The recommended alternative is to have each remote Allégro send its stream to the Application Server, and then have these streams relayed over the local network to the operators' client workstations.

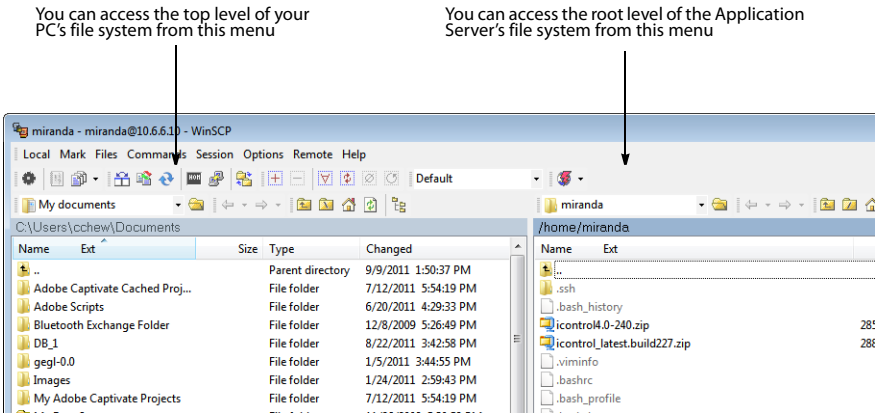
On the Application Server, for each Allégro in the configuration, you will need to create a file that provides some important parameters.

To configure streaming relays

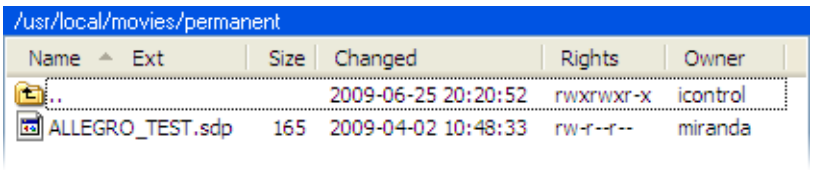
1. Launch WinSCP. If you do not have WinSCP installed on your PC or laptop, see "Installing WinSCP", on page 125.
2. Log on to the Application Server (see "Logging on to an Application Server from WinSCP", on page 129).

> **Note:** Only user `root` is allowed to add or modify files in the specific directory where the streaming relay configuration files must be located. Be sure to log on as user `root` (default password is `icontrol`).

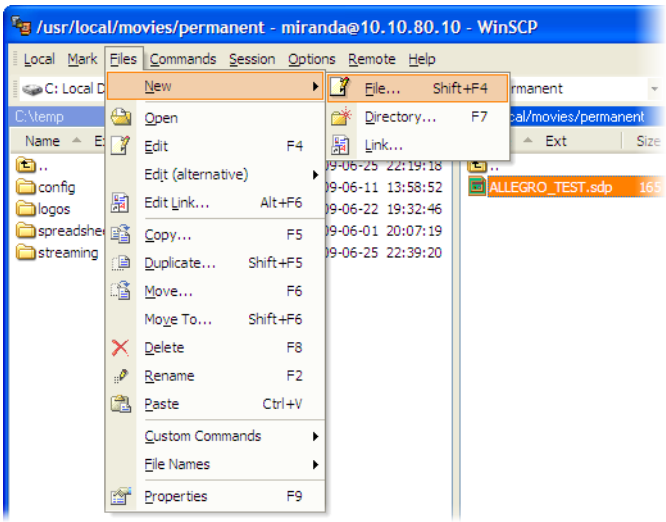
The main WinSCP window opens, showing the files on your PC in the left panel, and the files on the Application Server in the right panel.


You can access the top level of your PC's file system from this menu
You can access the root level of the Application Server's file system from this menu
miranda - miranda@10.6.6.10 - WinSCP
Local Mark Files Commands Session Options Remote Help
My documents
C:\Users\cchew\Documents
miranda
/home/miranda
Name Ext Size Type Changed
Adobe Captivate Cached Proj... File folder 7/12/2011 5:54:19 PM
Adobe Scripts File folder 6/20/2011 4:29:33 PM
Bluetooth Exchange Folder File folder 12/8/2009 5:26:49 PM
DB_1 File folder 8/22/2011 3:42:58 PM
gegl-0.0 File folder 1/5/2011 3:44:55 PM
Images File folder 1/24/2011 2:59:43 PM
My Adobe Captivate Projects File folder 7/12/2011 5:54:19 PM
.ssh
.bash_history
icontrol4.0-240.zip
icontrol_latest.build227.zip
.viminfo
.bashrc
.bash_profile

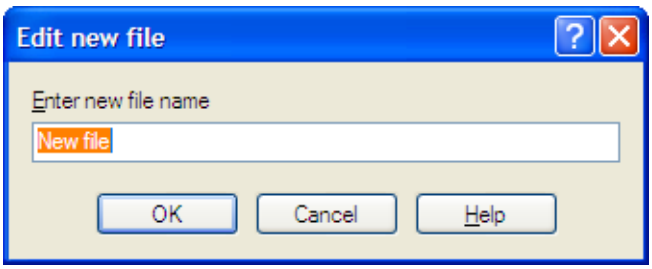
3. On the Application Server side, navigate to `/usr/local/movies/permanent`.


/usr/local/movies/permanent
Name Ext Size Changed Rights Owner
.. 2009-06-25 20:20:52 rwxrwxr-x icontrol
ALLEGRO_TEST.sdp 165 2009-04-02 10:48:33 rw-r--r-- miranda

4. On the **Files** menu, point to **New**, and then click **File**.



A window appears, prompting you for a file name.



5. Type a name, and then click **OK**.

> **Note:** The file name must match one of the names specified in the *Devices* tab of the configuration spreadsheet (see "Devices Worksheet", on page 86). For example, if this streaming relay corresponds to the device *Allegro1* in the spreadsheet, the file should be named `ALLEGRO1.sdp`.

6. Type (or copy and paste) the following into the new file:
   - `v=0`
   - `c=IN IP4 127.0.0.1`
   - `m=video 46010 RTP/AVP 96`
   - `a=rtpmap:96 MVC3/90000`
   - `a=control:trackID=6`
   - `m=audio 46012 RTP/AVP 1`
   - `a=rtpmap:1 MAC2/44100`
   - `a=control:trackID=7`
7. Change the port number in the third line (`46010` in the sample above) to a port number that is unique to this Allégro.

   > **Note:** This is the port that will be used for the video component of the streaming relay.

8. Change the port number in the sixth line (`46012` in the sample above) to a port number that is unique to this Allégro—usually the video component port number plus two; this is the port that will be used for the audio component of the streaming relay.

   > **Note:** The port numbers for the video and audio streaming components must be unique for each Allégro. As you create additional SDP files, increment the previously assigned port number by 4. For example, if the port numbers used in `ALLEGRO1.sdp` are `46010` and `46012`, then the port numbers used in `ALLEGRO2.sdp` should be `46014` and `46016`, and so on.

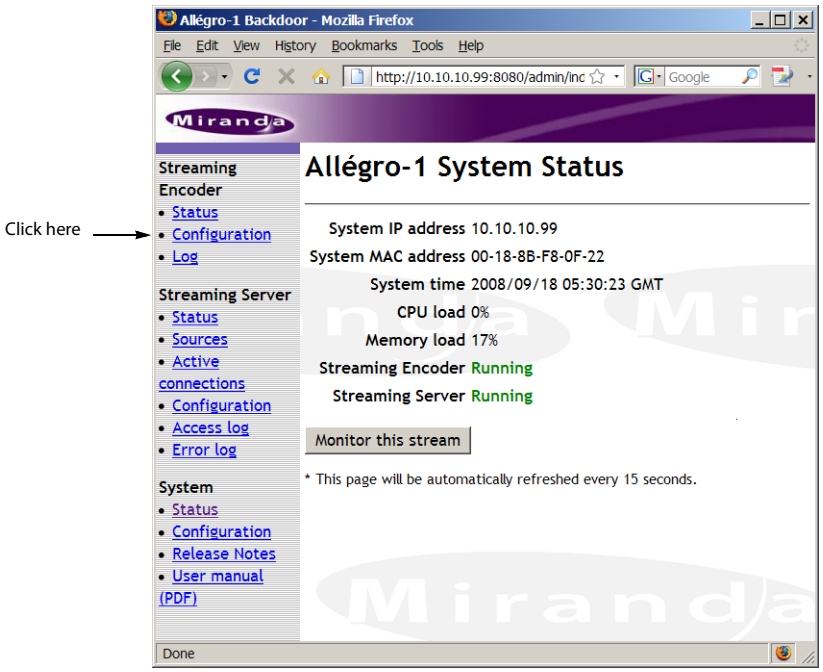
9. Save and close the file.
10. Repeat step 4 to step 9 for each Allégro in your configuration.

    Next, you must configure each Allégro so that it streams to the Application Server.

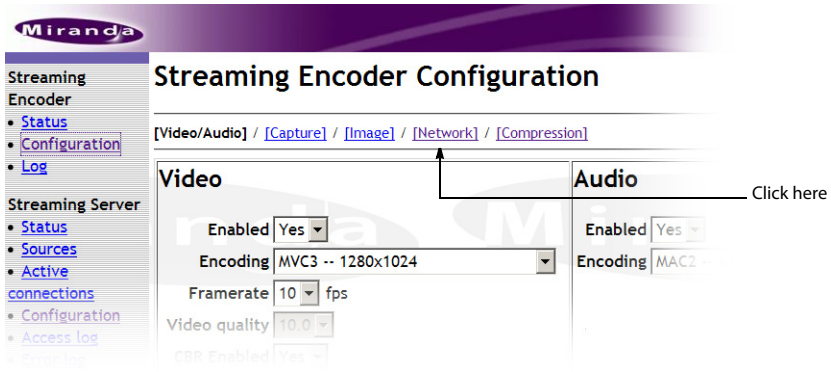
11. In your Web browser's address bar, type the Allégro's IP address and specify port 8080.

    (e.g. `http://10.44.34.25:8080`).

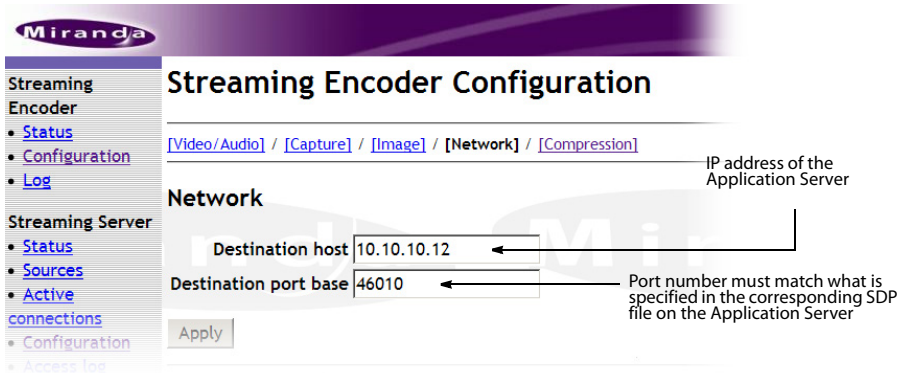
12. Under **Streaming Encoder**, click **Configuration**.



13. On the Streaming Encoder Configuration page, click **Network**.



14. On the Network page, type the Application Server's IP address in the **Destination host** box.



15. Type the appropriate port number in the **Destination port base** box (this number must match what is specified in the `ALLEGRO.sdp` file for this Allégro frame).
16. Click **Apply**.
17. Restart the Allégro.
18. Repeat step 11 to step 17 for each Allégro in the iControl Edge configuration.
19. Restart iControl on the Application Server.

Task 10: Verification & Readiness Check

When you finish configuring all devices, use an SSH client such as PuTTY to ping them from the Application Server to make sure that the devices recognize each other on your network.

> **Note:** PuTTY is available from your Application Server's Useful Downloads page. If you do not have PuTTY installed on your PC or laptop (see ."Installing PuTTY", on page 121).

To verify that all devices are properly connected to your system

1. Launch PuTTY and log on to the Application Server (see "Establishing an SSH Connection with an Application Server", on page 122).
2. In the PuTTY command line window, type the following:

   ```
   ping -s 32 AAA.BBB.CCC.DDD
   ```

   where `AAA.BBB.CCC.DDD` is the new IP address of a Global Caché GC-100 Network Adapter.

   A series of messages similar to the following should appear:

   ```
   PING 10.10.120.50 (10.10.120.50) 32(60) bytes of data.
   40 bytes from 10.10.120.50: icmp_seq=1 ttl=99 time=3.43 ms
   40 bytes from 10.10.120.50: icmp_seq=2 ttl=99 time=6.57 ms
   40 bytes from 10.10.120.50: icmp_seq=3 ttl=99 time=3.10 ms
   ```

   Notes

   - If the `ping` command is successful, stop the ping by pressing **Ctrl**+**C**.
   - If you see the message `Destination Host Unreachable`, stop the ping by pressing **Ctrl**+**C**, and then verify that the device is powered up, properly cabled, and that its IP address is correctly configured.

3. Repeat the previous step for every network device in your iControl Edge system (e.g. other GC-100 network adapters at this location, an Allégro system if one was installed at this location, other Application Servers if applicable).

   Notes

   - For a GC-100 Network Adapter, type: `ping -s 32 AAA.BBB.CCC.DDD`.
   - For any other device, simply type: `ping AAA.BBB.CCC.DDD`.

4. Type `exit`, and then press **Enter** to close the PuTTY command line window.

Task 11: Managing the iControl Edge Configuration Files

Two or more configuration spreadsheets are used to specify the network, audio channel, video channel and associated information for your iControl Edge network. The first spreadsheet, `Locations.xls`, is used to specify the physical locations (i.e. head ends) in your network. Each physical location corresponds to a separate spreadsheet containing multiple signal IDs that map to actual monitored channels. The signals, in turn, correspond to multiple signal paths that map to the physical path of the signal among different devices. In addition, you may need to create configuration files to define the commands that will be used by the Global Caché GC-100 Network Adapter to control your set-top boxes. A separate configuration file is needed for each specific set-top box model.

Creating Configuration files for the Global Caché GC-100 Network Adapter

Each Global Caché GC-100 Network Adapter that shipped with your system can control up to six different set-top boxes. Depending on the set-top box model, the set of supported IR signals may vary and follow different standards.

Your iControl Edge system includes a set of predefined configuration files for the following set-top box models:

Company	STB model	File name
ARION Technology	DVB STB model for Cablevision SA	ARION
Channel Master	CM-7000	ChannelMaster
Cisco (Scientific Atlanta)	Explorer 3250HD	Explorer3250HD
	Explorer 8240HDC	Explorer8240HDC
	Explorer 8550HDC	Explorer8550HDC
Echostar	Echostar 4100	Echostar4100
Kaon Media	Kaon DVB STB models for Cablevision SA	KAON_PAIDING, KAON_TC
Motorola	DCH3200	MotorolaDCH3200
	DCT700	MotorolaDCT700
	DCT3412, and DCT6416	MotorolaDCT3412
	DCT6412	MotorolaDCT6412
	DSR205	MotorolaDSR205
Philips	DTR 220	PhilipsDTR220
Scientific Atlanta	See *Cisco (Scientific Atlanta)*	
Winegard	RC-1010	WinegardRC1010

If you have other models of set-top boxes, you will need to create custom configuration files based on a template that is also located on the application server.

Notes

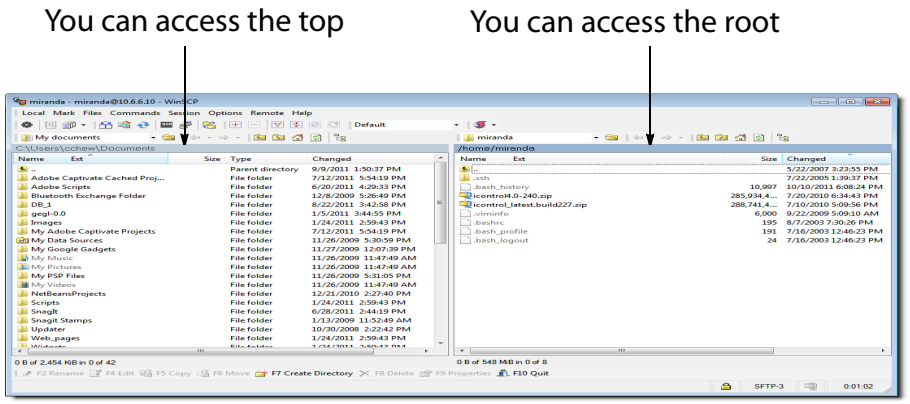
- Predefined configuration files for the GC-100 have a `.conf` file extension, and are located on the Application Server (under `var/tomcat4/webapps/icw/sites/EDGE/Config`).
- Customized configuration files must be uploaded to `/usr/local/iControl/bin/conf/GC100`.
- In the *Devices* worksheet, you must specify only the file name, but not the `.conf` extension (see "Devices Worksheet", on page 86).

Downloading the Configuration File Template from the Application Server

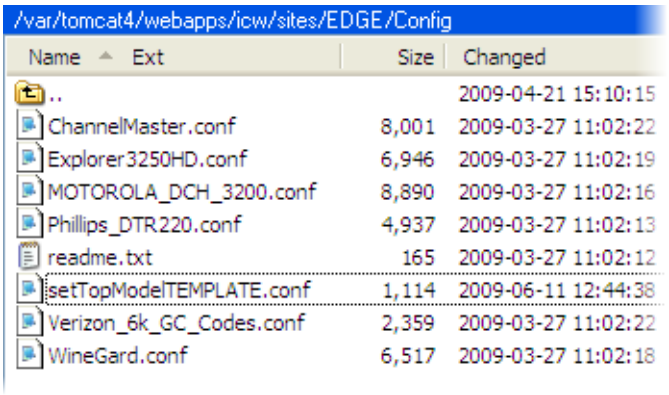
To download the configuration file template to your workstation

1. Launch WinSCP. If you do not have WinSCP installed on your PC, see "Installing WinSCP", on page 125.
2. Log on to the Application Server (see "Logging on to an Application Server from WinSCP", on page 129).

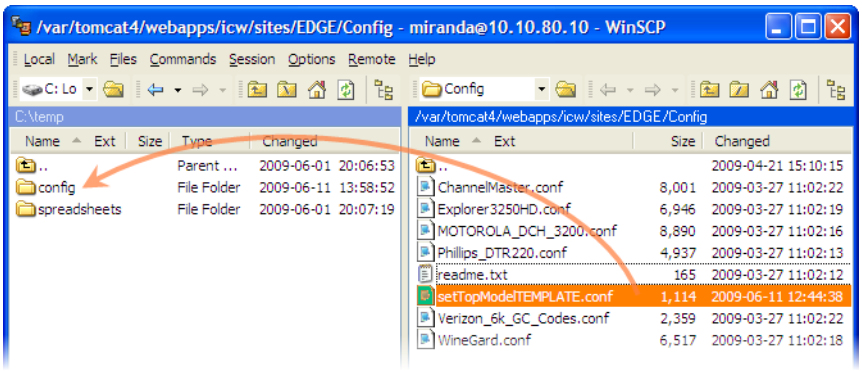
   The main WinSCP window opens, showing the files on your PC in the left panel, and the files on the Application Server in the right panel.



3. On the Application Server side, navigate to `/var/tomcat4/webapps/icw/sites/EDGE/Config`.



4. Select the configuration file template (`setTopModelTEMPLATE.conf`), and then drag it to a convenient location on your PC.


/var/tomcat4/webapps/icw/sites/EDGE/Config - miranda@10.10.80.10 - WinSCP
Local Mark Files Commands Session Options Remote Help
C:\temp
Name Ext Size Type Changed
.. Parent ... 2009-06-01 20:06:53
config File Folder 2009-06-11 13:58:52
spreadsheets File Folder 2009-06-01 20:07:19
/var/tomcat4/webapps/icw/sites/EDGE/Config
Name Ext Size Changed
.. 2009-04-21 15:10:15
ChannelMaster.conf 8,001 2009-03-27 11:02:22
Explorer3250HD.conf 6,946 2009-03-27 11:02:19
MOTOROLA_DCH_3200.conf 8,890 2009-03-27 11:02:16
Phillips_DTR220.conf 4,937 2009-03-27 11:02:13
readme.txt 165 2009-03-27 11:02:12
setTopModelTEMPLATE.conf 1,114 2009-06-11 12:44:38
Verizon_6k_GC_Codes.conf 2,359 2009-03-27 11:02:22
WineGard.conf 6,517 2009-03-27 11:02:18

   A confirmation window may appear.

5. Click **Copy** to continue.
6. Once the download has completed, close the main **WinSCP** window.

   If prompted, click **OK** to close the application.

   You have successfully downloaded a copy of the configuration file template. You can now proceed with populating this file with the required information, as described below (see "Capturing IR Codes from Remote Control Units", on page 80).

> **Note:** If you have more than one custom file to create, you may want to set aside a read-only copy of the template file on your hard drive to avoid having to download the clean template from the server again.

Capturing IR Codes from Remote Control Units

To capture the information required to recreate the IR signals that correspond to your specific set-top box models, you will need to use Global Caché - IR Learner Utility with the GC-IRL IR Learner serial device from Global Caché (see `http://www.globalcache.com/products/ir-index.html`).

> **Note:** The IR Learner Utility and more information are available from the *Support Documents and Files* section of Global Caché's Web site.
>
> See `http://www.globalcache.com/support/support_docs.html`.

To capture IR signals from the remote control unit associated with a specific set-top box model

1. Open a copy of the configuration file template in a text editor (e.g. Notepad).
2. Connect the GC-IRL IR Learner serial device to a serial port on your PC or laptop.
3. Launch the IR Learner Utility application (on the **Start** menu, point to **All Programs**, and then click **GC-IRL IR Learner Utility**).
4. In the **IR Learner Utility** window, select the following options:

Option	Value
End Timeout	100 ms
GC-100 Output	Selected
Repeat count	1
Module	2
Connector	1

5. Click **Connect** to connect the device to the PC application.
6. Use the set-top box remote control unit to point to the GC-IRL device, and then press one of the buttons on the remote (e.g. press 1).

   The IR signal from the remote is converted to a string of characters placed on the clipboard.
7. Paste the content of the clipboard into the template file on the line whose header corresponds to the button your pressed (e.g. `BUTTON_1`).

   The result will be something like the following:

   ```
   BUTTON_1 sendir,2:1,17,38000,1,1,341,171,21,63...
   ```
8. Repeat the same operation for every button on the remote control unit.
9. Save the text file, and name it after the set-top box model, with a `.conf` extension.

   > **Note:** The file name must not include spaces.
10. Close the text editor.
11. When you are done with editing configuration files and spreadsheets, you will need to upload them to the appropriate location on the server (see "Uploading and Applying iControl Edge Configuration Files", on page 108).

Downloading the iControl Edge Configuration Spreadsheets

The iControl Edge configuration spreadsheets reside on the Application Server. They can be downloaded for editing to a client PC or laptop with the Microsoft® Excel® spreadsheet software installed. You can use any suitable file transfer application (WinSCP, for instance) to download the spreadsheets.

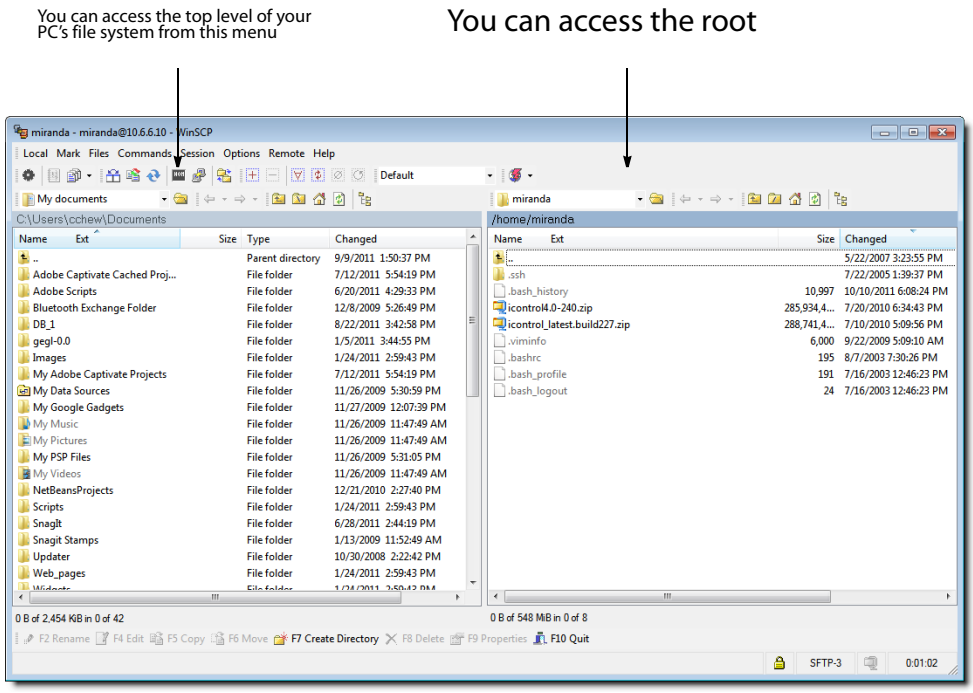
To download the iControl Edge configuration spreadsheets to your workstation

1. Launch WinSCP.

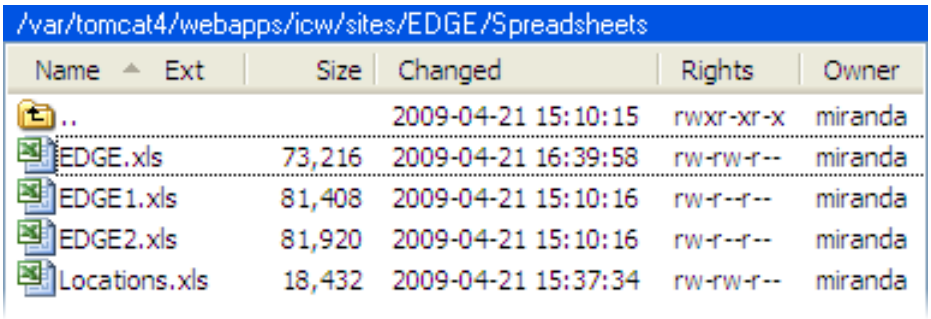
   If you do not have WinSCP installed on your PC or laptop, see "Installing WinSCP", on page 125.

2. Log on to the Application Server (see "Logging on to an Application Server from WinSCP", on page 129).

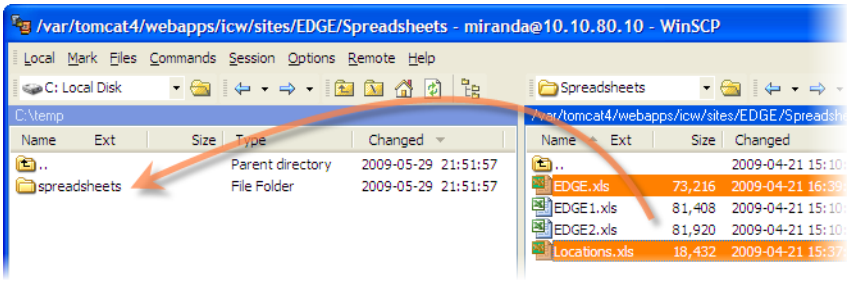
   The main WinSCP window opens, showing the files on your PC or laptop in the left panel, and the files on the Application Server in the right panel.


You can access the top level of your PC's file system from this menu
You can access the root
miranda - miranda@10.6.6.10 - WinSCP
Local Mark Files Commands Session Options Remote Help
C:\Users\cchew\Documents
/home/miranda

3. On the Application Server side, navigate to `/var/tomcat4/webapps/icw/sites/EDGE/Spreadsheets/`.


/var/tomcat4/webapps/icw/sites/EDGE/Spreadsheets
Name Ext Size Changed Rights Owner
.. 2009-04-21 15:10:15 rwxr-xr-x miranda
EDGE.xls 73,216 2009-04-21 16:39:58 rw-rw-r-- miranda
EDGE1.xls 81,408 2009-04-21 15:10:16 rw-r--r-- miranda
EDGE2.xls 81,920 2009-04-21 15:10:16 rw-r--r-- miranda
Locations.xls 18,432 2009-04-21 15:37:34 rw-rw-r-- miranda

4. Select the spreadsheet files (typically `Locations.xls` and `EDGE.xls`), and drag them to a convenient location on your PC or laptop.


/var/tomcat4/webapps/icw/sites/EDGE/Spreadsheets - miranda@10.10.80.10 - WinSCP
Local Mark Files Commands Session Options Remote Help
C: Local Disk
Spreadsheets
C:\temp
Name Ext Size Type Changed
.. Parent directory 2009-05-29 21:51:57
spreadsheets File Folder 2009-05-29 21:51:57
Name Ext Size Changed
.. 2009-04-21 15:10
EDGE.xls 73,216 2009-04-21 16:39
EDGE1.xls 81,408 2009-04-21 15:10
EDGE2.xls 81,920 2009-04-21 15:10
Locations.xls 18,432 2009-04-21 15:37

   A confirmation window may appear.

5. Click **Copy** to continue.
6. When you are done, close the main WinSCP window.
7. If prompted, click **OK** to close the application.

   You have successfully downloaded a copy of the configuration spreadsheets (see "Modifying the iControl Edge Configuration Spreadsheets", on page 83 for information on how to edit these files).

Modifying the iControl Edge Configuration Spreadsheets

You can edit the configuration spreadsheets on any client PC or laptop with the Microsoft® Excel® spreadsheet software installed. Once the files have been edited, you will transfer them back to the Application Server as described in "Uploading the iControl Edge Configuration Spreadsheets", on page 110.

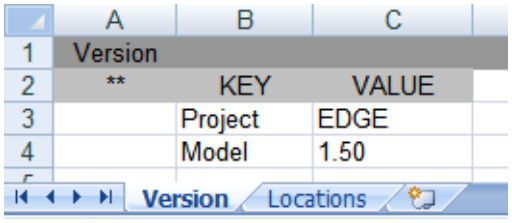
IMPORTANT: iControl Edge is Case-Sensitive to Data Entered in Spreadsheets.

Make sure all data entered into both spreadsheets

Note: Before editing a configuration spreadsheet, make a backup copy that can be used to restore the system to its previous state.

Locations Spreadsheet

When you open the `Locations.xls` file, you will see that it contains two worksheets, corresponding to the **Locations** and **Version** tabs at the bottom of the Excel window. The *Locations* worksheet contains data describing each of the remote locations that are part of your iControl Edge system. The *Version* worksheet determines how the *Devices* spreadsheets will be parsed throughout the system.



Locations Worksheet

To define the locations monitored in your iControl Edge configuration

1. Open the *Locations* spreadsheet in Excel, and then click the **Locations** tab.

   The *Locations* worksheet specifies the name of each location and associated *Devices* spreadsheet.

LOCATIONS								
**	ID	TYPE	ENABLE	SHORT NAME	LONG NAME	IP	HOSTNAME	SPREADSHEET
	LOCATION1	EDGE	YES	MTL	Montreal	10.10.80.10	EdgeAppServer	EDGE.xls
	LOCATION2	EDGE	YES	NY	New York	10.12.100.5	EdgeAppServNY	EDGE_NY.xls

   The table below describes the worksheet contents:

Column	Description
**	Two asterisks (**), with no spaces, positioned in the first column indicate rows to be ignored, such as rows containing column headers, or intended for future use.[1]
ID	The unique ID of the iControl Edge location. The current version of iControl Edge supports up to 12 locations. Mandatory.
TYPE	Must be `EDGE`.
ENABLE	Type `YES` to enable a location, `NO` to disable it for troubleshooting or maintenance. A disabled location remains defined in the system, but does not participate in monitoring/control operations. In the corresponding Web page, alarms associated with a disabled location will appear in black (i.e. their state will be considered unknown).
SHORT NAME	The short name of the location. Will be displayed at the bottom of the **Channel Selector** area (see the *Channel Selector* section in the *Web Monitoring* chapter of the *iControl Edge Operator's Overview*). Optional. On a typical system, the **Location** buttons can fit approximately 10 characters (or up to 16 characters, in the iControl Edge Web pages designed for a 1280 × 1024 display resolution). Longer names may appear truncated.

(*Continued*)

Column	Description
LONG NAME	The full name of the location. Will be displayed above the **Detailed Signal Analysis** area, and as a tooltip. Optional.
IP	IP address of the Application Server at this location. Mandatory.
HOSTNAME	Host name of the Application Server at this location. Must match the name specified under HOSTNAME for the Application Server, in the *Devices* worksheet for this location. Case sensitive. Mandatory.
SPREADSHEET	Name of the file that defines the monitoring devices available at this location. The names of the *Devices* spreadsheet files should be unique across the entire iControl Edge configuration (e.g. `EDGE1.xls`, `EDGE2.xls`, etc.). Mandatory.

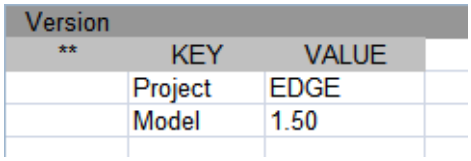
1. Rows you wish to leave empty must include the two asterisks in this column.

2. Add rows until there are enough to describe each location in your iControl Edge configuration.
3. For each row, specify an ID, a short name, a long name, the Application Server's IP address, its host name and the name of the corresponding spreadsheet file.

> **Note:** The short names appear on the **Location** buttons. On a typical system, the Location buttons can fit approximately 10 characters (or up to 16 characters, in the iControl Edge Web pages designed for a 1280 × 1024 display resolution). Longer names may appear truncated.

Version Worksheet

The iControl Edge configuration spreadsheets included with your initial purchase of an iControl Edge Application Server match the current version of the iControl Edge package. The set of spreadsheets provided with the next software release could have a different structure. However, when upgrading your iControl Edge system, you do not need to start over, and port all your existing data to the new spreadsheets. The Model attribute ensures that legacy spreadsheets can still be parsed with a new version of the package.



When you are ready to use the new features introduced with the most recent version of the package, then all you need to do is to add the necessary columns and rows to your existing spreadsheets, and populate them based on your actual system configuration. Once you have completed adding the new data, you must update the *Version* worksheet accordingly.

> **Note:** With the current version of the iControl Edge package, all locations within a distributed system must have configuration spreadsheets based on the same iControl Edge version.

To update the Model attribute in the Version worksheet

1. Open the *Locations* spreadsheet in Excel, and then click the **Version** tab.
2. On the **Tools** menu, point to **Protection**, and then click **Unprotect Sheet** to make the worksheet editable.

   > **Note:** By default, there is no password.

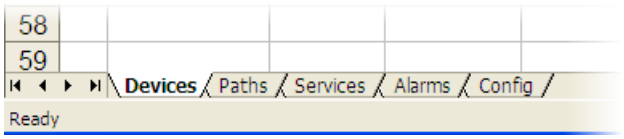
3. Update the Model value to the corresponding iControl Edge version number.
4. On the **Tools** menu, point to **Protection**, and then click **Protect Sheet** to make this worksheet read-only again.

   The **Protect Sheet** window appears.

5. Click **OK** to close it.

Devices Spreadsheet

When you open the `.xls` file that defines the monitoring devices available at a given location, you will see that it contains five worksheets—*Devices*, *Paths*, *Services*, *Alarms*, and *Config*—corresponding to tabs at the bottom of the Excel window.



Each worksheet contains data on various aspects of the iControl Edge configuration at this location. By editing the data, you can control the way your system operates.

Devices Worksheet

The *Devices* worksheet contains a list of the iControl Edge devices associated with a given location:

- Allégros
- Application Servers
- Densité frames
- Densité probes
- DVRs
- EdgeVision devices
- Global Caché GC-100 network adapters

- PDUs
- Set-top boxes

DEVICES							
**	APPLICATION SERVER						
**	ID	TYPE	ENABLE	IP	HOSTNAME		
	APPSERVER1	AS	YES	10.6.6.8	A8		
**	DENSITE						
**	ID	TYPE	ENABLE	NAME	APP SERVER ID		
	DENSITE1	DENSITE	YES	Densitay	APPSERVER1		
**	ALLEGRO	(STREAMER)					
**	ID	TYPE	ENABLE	IP			
	ALLEGRO1	ALLEGRO	YES	10.6.6.42			
**	PDU						
**	ID	TYPE	ENABLE	IP	APP SERVER ID		
**	PDU_HUB_A	APC7900	YES	10.6.6.9	APPSERVER1		
**	CARD	(PHYSICAL PROBE)					
**	ID	TYPE	ENABLE	DENSITE ID	SLOT		
	CARD1	DEC1023	YES	DENSITE1	5		
	CARD2	UAP1781	YES	DENSITE1	2		
**	GC100						
**	ID	TYPE	ENABLE	IP	PORT	APP SERVER ID	
	GC1001	GC100	YES	10.6.6.41	4998	APPSERVER1	
**	GC100 IR PORT						
**	ID	TYPE	ENABLE	GC100 ID	PORT	STB	REMOTE CONTROL PAGE
	GC1001_PORT1	GC100_PORT	YES	GC1001	1	Explorer3250HD	

Devices worksheet (part 1)

**	EDGEVISION							
**	ID	TYPE	ENABLE	IP	UNIT NAME			
	EDGEVISION1	EDGEVISION	YES	10.6.6.43	EV43			
**	EDGEVISION INPUT	(IR CONTROLLER / PHYSICAL PROBE / STREAMER)						
**	ID	TYPE	ENABLE	EDGEVISION ID	INPUT			
	EDGEVISION1_INPUT1	EDGEVISION_INPUT	YES	EDGEVISION1	1			
	EDGEVISION1_INPUT2	EDGEVISION_INPUT	YES	EDGEVISION1	2			
**	STBTUNER	(IR CONTROLLER)						
**	ID	TYPE	ENABLE	IR CONTROLLER PORT		PDU ID	PDU OUTLET	
	EV_TUNER1	STBTUNER	YES	EDGEVISION1_INPUT1				
	GC_TUNER2	STBTUNER	YES	GC1001_PORT1				
**	DVRTUNER	(IR CONTROLLER)						
**	ID	TYPE	ENABLE	IR CONTROLLER PORT	ELECTRONIC PROGRAM GUIDE	PDU ID	PDU OUTLET	RECORD DURATION
	DVRTUNER1	DVRTUNER	YES	EDGEVISION1_INPUT2				60
**	VIRTUAL DEVICE	(VIRTUAL PROBE)						
**	ID	TYPE	ENABLE	PHYSICAL PROBE ID	CYCLER ID			
	VIRTUAL1	VIRTUAL	YES	EDGEVISION1_INPUT1	CYCLER1			
	VIRTUAL2	VIRTUAL	YES	CARD1	CYCLER2			
	VIRTUAL3	VIRTUAL	YES	CARD2	CYCLER2			
**	CYCLER							
**	ID	TYPE	ENABLE	POLLING PERIOD	SETTLING TIME	DURATION	OCCURRENCES	
	CYCLER1	CYCLER	YES	45000	5000	30000	1	
	CYCLER2	CYCLER	YES	45000	5000	30000	1	

Devices worksheet (part 2)

This worksheet also includes a section where virtual devices are defined. A virtual device is an abstract concept, that associates a physical Densité card to a cycler profile.

The last section at the bottom of this worksheet is the *Cycler* section where the necessary cycler profiles are configured.

Table 3-3, below, describes the worksheet contents (column headings listed alphabetically):

Table 3-3: Devices worksheet contents

Area	Column	Description
• APPLICATION SERVER • DENSITE • ALLEGRO (STREAMER) • PDU • CARD (PHYSICAL PROBE) • GC100 • GC100 IR PORT • EDGEVISION • EDGEVISION INPUT (IR CONTROLLER / PHYSICAL PROBE / STREAMER) • STBTUNER (IR CONTROLLER) • DVRTUNER (IR CONTROLLER) • VIRTUAL DEVICE (VIRTUAL PROBE) • CYCLER	**	Two asterisks (**), with no spaces, are positioned in the first column to indicate rows to be ignored, such as rows containing column headers, or intended for future use.[1]
	ID	The unique indentifier for the device. This ID is used to reference the device within and between spreadsheets. Mandatory.
	ENABLE	Type `YES` to enable a device, `NO` to disable it for troubleshooting or maintenance. A disabled device remains defined in the system, but does not participate in monitoring/control operations. In the corresponding Web page, alarms associated with a disabled device will appear in black (i.e. their state will be considered unknown).
	TYPE	The device type. Choices are: • `AAP1741` = AAP-1741 4-Channel Analog Audio Processor • `ACP1721` = ACP-1721 Digital Audio Control Probe • `ALLEGRO` = Allégro Streaming Encoder/Server • `AS` = Application Server • `CYCLER` = Defines a cycling profile and associated alarm debouncing parameters • `DEC1002` = DEC-1002 10-Bit Composite to SDI Decoder • `DEC1003` = DEC-1003 10-Bit Composite to SDI Decoder with Probing Option • `DEC1023` = DEC-1023 12-Bit 3D Composite to SDI Decoder with Probing • `DENSITE` = Densité Housing Frame • `DVR` = Digital Video Recorder • `DVRTUNER` = Set-Top Box model with a recording time parameter • `EDGEVISION` = Physical EdgeVision device • `EDGEVISION_INPUT` = EdgeVision input port (conceptually the same as a Densité frame slot) • `GC100` = Global Caché GC-100 Network Adapter • `HCP1801` = HCP-1801 HD/SD Video Control Probe with Embedded Audio • `SCP-1121` = SDI Control Probe with Embedded Audio • `STB` = Set-Top Box • `STBTUNER` = Set-Top Box model • `UAP1781` = UAP-1781 8-Channel Universal Audio Processor • `UAP1783` = UAP-1783 8-Channel Universal Audio Processor • `VCP1021` = VCP-1021 Composite Control Probe • `VIRTUAL` = Represents a Densité probe and the associated cycling profiles Mandatory.
• DENSITE • PDU • GC100	APP SERVER ID	ID of the associated Application Server (e.g. `APPSERVER1`). Case sensitive. Mandatory.
VIRTUAL DEVICE (VIRTUAL PROBE)	CYCLER ID	ID of the cycler associated with a specific probe.[2]

Table 3-3: Devices worksheet contents (*Continued*)

Area	Column	Description
CARD (PHYSICAL PROBE)	DENSITE ID	ID of the associated Densité frame (e.g. `DENSITE1`).
EDGEVISION INPUT (IR CONTROLLER / PHYSICAL PROBE / STREAMER)	EDGEVISION ID	ID of the EdgeVision device associated with a particular EdgeVision Input port.
EDGEVISION INPUT (IR CONTROLLER / PHYSICAL PROBE / STREAMER)	INPUT	Numerical port designation for a specific Input port of an EdgeVision device.
• APPLICATION SERVER • ALLEGRO (STREAMER) • PDU • GC100 • EDGEVISION	IP	Unique IP address of the device. Mandatory.
• STBTUNER (IR CONTROLLER) • DVRTUNER (IR CONTROLLER)	IR CONTROLLER PORT	The infra-red controller port device ID. This may be a GC100 port or an EdgeVision input.
	PDU ID	ID of the PDU (power distribution unit) powering this device
	PDU OUTLET	PDU outlet number being used by this device
APPLICATION SERVER	HOSTNAME	Host name of the Application Server. Case sensitive. Mandatory.
DENSITE	NAME	The name of a Densité frame.
CYCLER	OCCURRENCES	Number of alarm occurrences required before an alarm is triggered. Default value: `1`
	POLLING PERIOD	Total length, in milliseconds, of the period allowed for monitoring each channel during a cycle, including the settling phase, and the listening phase. Default value is `45000 ms`, i.e. 45 seconds.
	DURATION	Determines the amount of time, in milliseconds, required before an error condition is considered as an alarm occurrence. Default value is `30000 ms`, i.e. 30 seconds.[3]
	SETTLING TIME	Time allowed, in milliseconds, at the beginning of each polling period for properly tuning a channel. Alarms are not actively monitored during this period. Default value is `5000 ms`, i.e. 5 seconds.
GC100	PORT	Active port number on a GC-1O0 network adapter. Must be `4998`.
VIRTUAL DEVICE (VIRTUAL PROBE)	REAL DEVICE ID	ID of the Densité probe associated with a specific virtual service.

Table 3-3: Devices worksheet contents (*Continued*)

Area	Column	Description
DVRTUNER (IR CONTROLLER)	RECORD DURATION	Maximum time during which the associated DVR will record a video stream after an error is detected. Default value is `60 seconds`.
	ELECTRONIC PROGRAM GUIDE	The electronic program guide related to the macros.
GC100 IR PORT	REMOTE CONTROL PAGE	Path to an iC Web page (MPF file) that represents the remote control used with a specific set-top box (or DVR) model, relative to EDGE/Web_pages. A set of default MPF files is provided matching the remotes commonly used with the set-top models for which a predefined configuration file (for the GC-100) exists. If left blank, a generic remote control image will be used.
	STB	Specific remote control model associated with a specific device.
	GC100 ID	ID of the GC-100 network adapter associated with a specific set-top box.
	PORT	IR output port number (1-6) on the GC-100 from which commands are sent to a specific set-top box.
CARD (PHYSICAL PROBE)	SLOT	Slot number (1-20) where the card is located inside the associated Densité frame.
EDGEVISION	UNIT NAME	A user-defined name of an EdgeVision device.

1. Rows you wish to leave empty must include the two asterisks in this column.
2. Specify the same cycler ID for each pair of audio and video probes: a pair of probes that are meant to process video and audio signals from the same channel must be associated with the same cycler ID.
3. This value should be less than the length of the polling period minus the settling time.

To define the devices at this location

1. Click the **Devices** tab.
2. In the *APPLICATION SERVER* area, perform the following sub-steps **for each Application Server in your iControl Edge setup**:

   IMPORTANT: Do not deviate from the default values for *TYPE* (`AS`), or *ENABLE* (`YES`).

   a) In the *ID* column of the first blank row, specify an ID string for the Application Server.
   b) In the *IP* column, in the same row, specify the Application Server's IP address (see "Configuring the Ethernet Interface", on page 37).
   c) In the *HOSTNAME* column, in the same row, specify the Application Server's host name and host name (see "Specifying DNS Client Settings", on page 33).
3. In the *DENSITE* area, perform the following sub-steps **for each Densité frame**:

   IMPORTANT: Do not deviate from the default values for *TYPE* (`DENSITE`), or *ENABLE* (`YES`).

   a) In the *ID* column of the first blank row, specify the ID string for the Densité frame.

   Note: The ID for each Densité frame across the entire iControl Edge configuration should be unique (e.g. `Densite1`, `Densite2`, etc.).

b) In the *NAME* column, in the same row, specify this Densité frame's host name (see "Configuring Densité Services", on page 55).

c) In the *APP SERVER ID* column, in the same row, specify the ID of the associated Application Server for this Densité frame.

4. In the *ALLEGRO (STREAMER)* area, perform the following sub-steps **for each Allégro device**:

IMPORTANT: Do not deviate from the default values for *TYPE* (`ALLEGRO`), or *ENABLE* (`YES`).

a) In the *ID* column of the first blank row, specify the ID string for the Allégro-1 device.

Note: The ID for each Allégro across the entire iControl Edge configuration should be unique (e.g. `Allegro1`, `Allegro2`, etc.).

b) In the *IP* column, in the same row, specify this Allégro's IP address.

Note: If the Application Server is configured to relay for the Allégro stream (see "Configuring Allégro Streaming Relays", on page 73), you must put the Application Server's ID in the APP *SERVER ID* column, beside the Allégro's IP address.

5. In the *PDU* area, perform the following sub-steps **for each APC7900 PDU**:

Note: Currently, the APC7900 PDU is the only network-reachable PDU supported in iControl Edge.

IMPORTANT: Do not deviate from the default values for *TYPE* (`APC7900`), or *ENABLE* (`YES`).

a) In the *ID* column of the first blank row, specify an ID string for the APC7900.

b) In the *IP* column, in the same row, specify the IP address of the APC7900.

c) In the *APP SERVER ID* column, in the same row, specify the ID of the Application Server (entered in step 2).

6. In the *CARD (PHYSICAL PROBE)* area, perform the following sub-steps **for each Densité card**:

IMPORTANT: Do not deviate from the default values for *TYPE* (unique for each card type), or *ENABLE* (`YES`).

a) In the *ID* column of the first blank row, specify an ID string for this Densité card.

Note: The ID for each Densité card across the entire iControl Edge configuration should be unique (e.g. `Card1`, `Card2`, etc.).

b) In the *TYPE* column, in the same row, specify this card's type.

c) In the *DENSITE ID* column, in the same row, specify the ID for the associated Densité frame (see "Configuring Densité Services", on page 55).

d) In the *SLOT* column, in the same row, specify the Densité frame slot number in which this card is seated.

7. In the *GC100* area, perform the following sub-steps **for each GC-100 at this location**:

IMPORTANT: Do not deviate from the default values for *TYPE* (GC100), *ENABLE* (YES), and *PORT* (4998).

a) In the *ID* column of the first blank row, specify an ID string for the GC-100 network adapter.

Note: The ID for each GC-100 network adapter across the entire iControl Edge configuration should be unique (e.g. GC1001, GC1002, etc.).

b) In the *IP* column, in the same row, specify this GC-100 network adapter's IP address.

c) In the *APP SERVER ID* column, in the same row, specify the associated Application Server's ID.

8. In the *GC100 IR PORT* area, perform the following sub-steps **for each infrared port of each GC100 network adapter device**:

IMPORTANT: Do not deviate from the default values for *TYPE* (GC100_PORT), *ENABLE* (YES), and *GC100 ID* (GC1001).

a) In the *ID* column of the first blank row, specify an ID string for the IR port of the associated GC-100 device.

b) In the *PORT* column, in the same row, specify the port number of this IR port.

c) In the *STB* column, in the same row, specify the specific remote control device associated with the appropriate STB device.

d) If an iC Web page (MPF file) exists on the Application Server under EDGE/Web_pages, representing the desired remote control used with a specific set-top box or DVR model, enter this file name in the *REMOTE CONTROL PAGE* column.

Notes

- Type the exact file name of the Web page into this cell of the worksheet (e.g. RemoteControl_Elegants_4400.mpf).
- If you leave the *REMOTE CONTROL PAGE* cell blank, iControl Edge will display the generic remote control.

9. If you are using one or more EdgeVision devices in your setup, in the *EDGEVISION* area, perform the following sub-steps **for each EdgeVision device**:

IMPORTANT: Do not deviate from the default value for *TYPE* (EDGEVISION).

a) In the *ID* column of the first blank row, specify an ID string for the EdgeVision device.

b) In the *ENABLE* column, in the same row, type YES.

Note: If at any time you would like to temporarily disable the device, do so by typing NO in this cell of the spreadsheet.

c) In the *IP* column, in the same row, type the IP address of the EdgeVision device.

d) In the *UNIT NAME* column, in the same row, type the unit name for this EdgeVision device.

Note: The unit name is retrievable from the EdgeVision Admin page.

10. If you are using one or more EdgeVision devices in your setup, in the *EDGEVISION INPUT (IR CONTROLLER / PHYSICAL PROBE / STREAMER)* area, perform the following sub-steps **for each input port of each EdgeVision device**:

IMPORTANT: Do not deviate from the default value for *TYPE* (`EDGEVISION_INPUT`).

Note: For the EDGEVISION INPUT area, the remote control device information for your STB is retrieved from the EdgeVision device.

a) In the *ID* column of the first blank row, specify an ID string for the input port.
b) In the *ENABLE* column, in the same row, type `YES`.
c) In the *EDGEVISION ID* column, in the same row, specify the ID of the EdgeVision device this port belongs to.
d) In the *INPUT* column, in the same row, specify the port number of this input port.

11. In the *STBTUNER (IR CONTROLLER)* area, perform the following sub-steps **for each STB**:

IMPORTANT: Do not deviate from the default values for *TYPE* (`STBTUNER`) or *ENABLE* (`YES`).

Note: iControl Edge continues to support the `STB` type (along with the new `STBTUNER` type). The difference is that `STBTUNER` supports PDU power cycling and `STB` does not.

a) In the *ID* column of the first blank row, specify an ID string for the STB tuner.

Note: The ID for each tuner across the entire iControl Edge configuration should be unique (e.g. `EV_TUNER1`, `STBTUNER2`, etc.).

b) In the *IR CONTROLLER PORT* column, in the same row, specify the IR controller input port associated with this STB tuner.
c) In the *PDU ID* column, in the same row, specify the ID of the power distribution unit (PDU) serving this tuner.
d) In the *PDU OUTLET* column, in the same row, specify the PDU outlet number serving this tuner.

12. In the *DVRTUNER (IR CONTROLLER)* area, perform the following sub-steps **for each DVR**:

IMPORTANT: Do not deviate from the default value for *TYPE* (`DVR`) or *ENABLE* (`YES`).

Note: iControl Edge continues to support the `DVR` type (along with the new `DVRTUNER` type). The difference is that `DVRTUNER` supports PDU power cycling and `DVR` does not.

a) In the *ID* column of the first blank row, specify an ID string for the DVR.

> **Note:** The ID for each DVR across the entire iControl Edge configuration should be unique (e.g. `DVR1`, `DVR2`, etc.).

b) In the *IR CONTROLLER PORT* column, in the same row, specify the IR controller input port associated with this DVR.

c) In the *ELECTRONIC PROGRAM GUIDE* column, in the same row, specify the JavaScript function prefix of the recording macro associated with this DVR (see "Retrieving a DVR's Recording Macro Prefix", on page 95).

d) In the *PDU ID* column, in the same row, specify the ID of the power distribution unit (PDU) serving this tuner.

e) In the *PDU OUTLET* column, in the same row, specify the PDU outlet number serving this tuner.

f) In the *RECORD DURATION* column, in the same row, specify the maximum time during which the associated DVR will record a video stream after an error is detected.

13. In the *VIRTUAL DEVICE (VIRTUAL PROBE)* area, perform the following sub-steps **for each virtual device**:

> **IMPORTANT:** Do not deviate from the default values for *TYPE* (`VIRTUAL`) or *ENABLE* (`YES`).

a) In the *ID* column of the first blank row, specify an ID string representing either a Densité card or an EdgeVision input that will probe signals from a cycling set-top box.

> **Note:** The ID for each virtual device across the entire iControl Edge configuration should be unique (e.g. `VIRTUAL1`, `VIRTUAL2`, etc.).

b) In the *REAL DEVICE ID* column, in the same row, specify the associated Densité card ID or EdgeVision Input port.

c) In the *CYCLER ID* column, in the same row, specify a common cycler ID for each pair of audio and video probes (i.e. a pair of probes that are meant to process video and audio signals from the same channel must be associated with the same cycler ID).

14. In the *CYCLER* area, perform the following sub-steps **for each cycler listed in the VIRTUAL DEVICE section**:

> **IMPORTANT:** Do not deviate from the default values for *TYPE* (`CYCLER`) or *ENABLE* (`YES`).

a) In the ID column of the first blank row, specify an ID string for the cycler (see step 13).

b) In the *POLLING PERIOD* column, in the same row, specify the appropriate polling period for the channel lineup that will be associated with a given cycling set-top box.

c) In the *SETTLING TIME* column, in the same row, specify the appropriate settling time (in seconds) for the channel lineup that will be associated with a given cycling set-top box.

d) In the *DURATION* and *OCCURRENCES* columns, in the same row, specify appropriate alarm debouncing parameters for this cycler.

Notes

- A cycle consists of two phases: the settling phase, and the listening phase (polling period).
- Alarms are actively monitored during the listening phase only. When an alarm condition is detected - if it lasts at least for the duration specified - then it is counted as a single occurrence.
- The specified duration should be less than the polling period minus the settling time.
- The number of occurrences can span more than one cycle.

Retrieving a DVR's Recording Macro Prefix

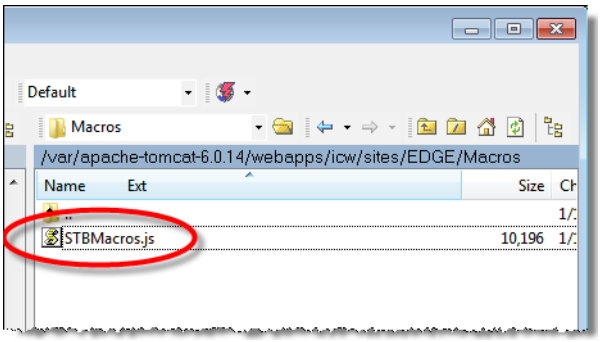
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

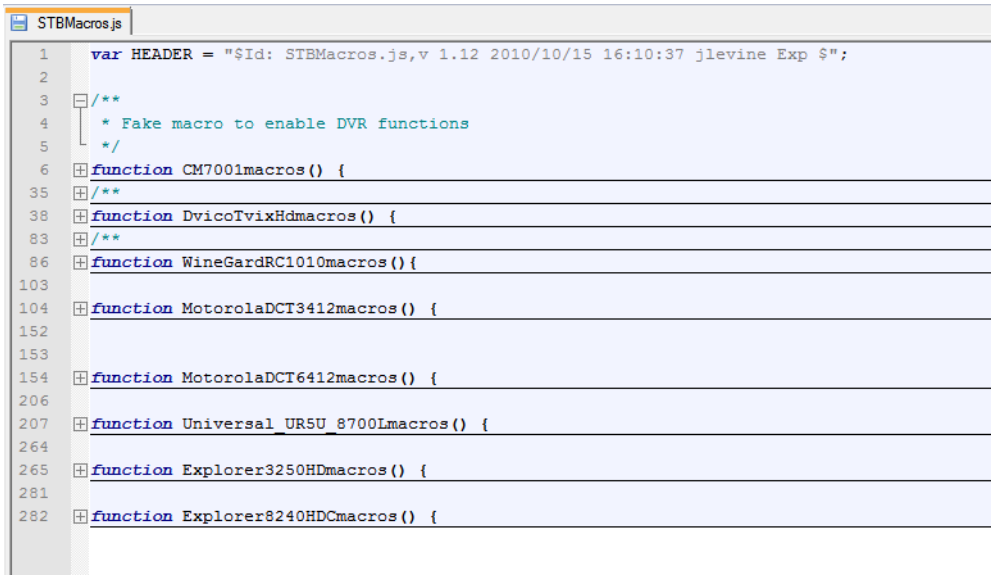
- You have downloaded WinSCP onto your client PC (see "Using WinSCP", on page 125).
- You have a text editor on your client PC.

To retrieve a DVR's recording macro prefix

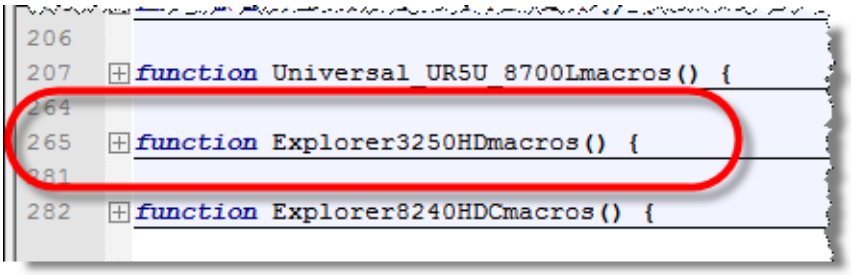
1. Using WinSCP, copy the `STBMacros.js` file from the `EDGE/Macros` directory on the Application Server.



2. Using a text editor, open `STBMacros.js`.
3. If you are using an advanced text editor like Notepad++, collapse all JavaScript functions until you are able to see all functions at once.



4. Identify the function associated with your DVR.



5. Take note of the name of the function.

   The prefix is the function name **without** the `macros()` ending. In this case, it is `Explorer3250HD`.

Paths Worksheet

For a given location, the *Paths* worksheet specifies which set-top box feeds which Densité modules (usually a pair of audio/video probes represented as virtual devices associated with a common cycling profile; see "Devices Worksheet" , step 13), and whether an EdgeVision or Allégro is used for streaming signals from a designated set-top box.

PATHS								
**	CYCLER PATHS (VIRTUAL)							
**	ID	TYPE	ENABLE	IR CONTROLLER ID	VIRTUAL VIDEO PROBE ID	VIRTUAL AUDIO PROBE ID		
	C_PATH1	STB_CYCLING	YES	EV_TUNER1	VIRTUAL1	VIRTUAL1		
	C_PATH2	STB_CYCLING	YES	GC_TUNER2	VIRTUAL2	VIRTUAL3		
**	MANUAL PATHS (PHYSICAL)							
**	ID	TYPE	ENABLE	IR CONTROLLER ID	ACTUAL VIDEO PROBE ID	ACTUAL AUDIO PROBE ID	RESERVED	STREAMER ID
	M_PATH1	STB_MANUAL	YES	DVRTUNER1	EDGEVISION1_INPUT2	EDGEVISION1_INPUT2		EDGEVISION1_INPUT2

IMPORTANT: System behavior

If, in the *MANUAL PATHS (PHYSICAL)* area, the *ACTUAL VIDEO PROBE ID* and *ACTUAL AUDIO PROBE ID* cells are left blank, the alarm panel of the **Detail Viewer** displays a *snapshot* of alarm states from when the service was last cycled. If, instead, probe IDs are specified, a probe populates the alarm panel in real time.

Note: The video/audio probe IDs in the *CYCLER PATHS (VIRTUAL)* area differ from the probe IDs of the *MANUAL PATHS (PHYSICAL)* area because cyclers use virtual devices. The physical probe is shared among all services in the cycler. By contrast, the Manual path must specify a physical probe ID because it is not virtual.

The table below describes the *Paths* worksheet contents:

Table 3-4: Paths worksheet contents

Area	Column	Description
• CYCLER PATHS (VIRTUAL) • MANUAL PATHS (PHYSICAL)	**	Two asterisks (**), with no spaces, are positioned in the first column to indicate rows to be ignored, such as rows containing column headers, or intended for future use.[1]
	ID	The unique indentifier for the path. This ID is used to reference the device within and between spreadsheets. Mandatory.
	TYPE	The device type. Mandatory. Choices are: • `STB_CYCLING` = Set-top box (or DVR) controlled by a cycler service • `STB_MANUAL` = manually-controlled set-top box (or DVR)
	ENABLE	Type `YES` to enable a Path, `NO` to disable it for troubleshooting or maintenance.
	IR CONTROLLER ID	Unique ID of a set-top box or DVR, as specified on the *Devices* worksheet. Case sensitive. Mandatory.
CYCLER PATHS (VIRTUAL)	VIRTUAL VIDEO PROBE ID	Unique ID of a video probe, as specified on the *Devices* worksheet. Case sensitive. Mandatory in cycling paths. Optional in manual paths.
	VIRTUAL AUDIO PROBE ID	Unique ID of an audio probe, as specified on the *Devices* worksheet. Case sensitive. Optional.

Table 3-4: Paths worksheet contents (*Continued*)

Area	Column	Description
MANUAL PATHS (PHYSICAL)	ACTUAL VIDEO PROBE ID	Unique ID of a video probe, as specified on the *Devices* worksheet. Case sensitive. Mandatory in cycling paths. Optional in manual paths.
	ACTUAL AUDIO PROBE ID	Unique ID of an audio probe, as specified on the *Devices* worksheet. Case sensitive. Mandatory in cycling paths. Optional in manual paths.
	STREAMER ID	Unique ID of the streaming device, as specified on the *Devices* worksheet. Case sensitive. Mandatory.

1. Rows you wish to leave empty must include the two asterisks in this column.

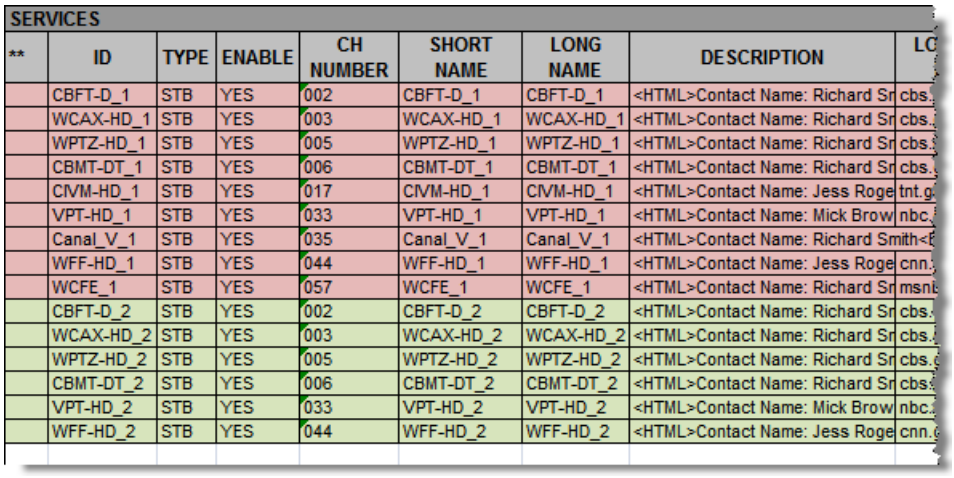
To define the signal paths for this site

1. Click the **Paths** tab.
2. For each path, specify a unique ID, and the *TYPE* of device being used in the path (`STB_CYCLING` or `STB_MANUAL`).
3. Specify the associated *IR CONTROLLER ID*.
4. For a cycling path, specify the virtual device IDs representing the associated pair of video and audio probes.
5. For a manual path, specify the card IDs representing the associated pair of video and audio probes, if present.

> **Note:** In the case of HCP-1801 HD/SD video control probes with embedded audio, both VIRTUAL VIDEO PROBE ID and VIRTUAL AUDIO PROBE ID should refer to the same virtual device ID, and both ACTUAL VIDEO PROBE ID and ACTUAL AUDIO PROBE ID should refer to the same physical card ID.

Services Worksheet

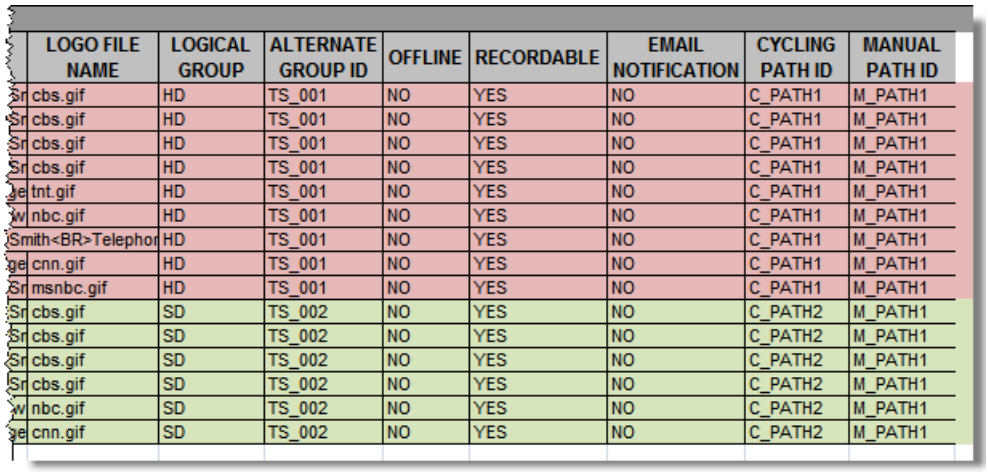
The *Services* worksheet is used to define the services or channels assigned to a path:



SERVICES

**	ID	TYPE	ENABLE	CH NUMBER	SHORT NAME	LONG NAME	DESCRIPTION	LC
	CBFT-D_1	STB	YES	002	CBFT-D_1	CBFT-D_1	<HTML>Contact Name: Richard Sr	cbs.
	WCAX-HD_1	STB	YES	003	WCAX-HD_1	WCAX-HD_1	<HTML>Contact Name: Richard Sr	cbs.
	WPTZ-HD_1	STB	YES	005	WPTZ-HD_1	WPTZ-HD_1	<HTML>Contact Name: Richard Sr	cbs.
	CBMT-DT_1	STB	YES	006	CBMT-DT_1	CBMT-DT_1	<HTML>Contact Name: Richard Sr	cbs.
	CIVM-HD_1	STB	YES	017	CIVM-HD_1	CIVM-HD_1	<HTML>Contact Name: Jess Roge	tnt.g
	VPT-HD_1	STB	YES	033	VPT-HD_1	VPT-HD_1	<HTML>Contact Name: Mick Brow	nbc.
	Canal_V_1	STB	YES	035	Canal_V_1	Canal_V_1	<HTML>Contact Name: Richard Smith<	
	WFF-HD_1	STB	YES	044	WFF-HD_1	WFF-HD_1	<HTML>Contact Name: Jess Roge	cnn.
	WCFE_1	STB	YES	057	WCFE_1	WCFE_1	<HTML>Contact Name: Richard Sr	msnb
	CBFT-D_2	STB	YES	002	CBFT-D_2	CBFT-D_2	<HTML>Contact Name: Richard Sr	cbs.
	WCAX-HD_2	STB	YES	003	WCAX-HD_2	WCAX-HD_2	<HTML>Contact Name: Richard Sr	cbs.
	WPTZ-HD_2	STB	YES	005	WPTZ-HD_2	WPTZ-HD_2	<HTML>Contact Name: Richard Sr	cbs.
	CBMT-DT_2	STB	YES	006	CBMT-DT_2	CBMT-DT_2	<HTML>Contact Name: Richard Sr	cbs.
	VPT-HD_2	STB	YES	033	VPT-HD_2	VPT-HD_2	<HTML>Contact Name: Mick Brow	nbc.
	WFF-HD_2	STB	YES	044	WFF-HD_2	WFF-HD_2	<HTML>Contact Name: Jess Roge	cnn.

Services worksheet (part 1)



	LOGO FILE NAME	LOGICAL GROUP	ALTERNATE GROUP ID	OFFLINE	RECORDABLE	EMAIL NOTIFICATION	CYCLING PATH ID	MANUAL PATH ID
Sr	cbs.gif	HD	TS_001	NO	YES	NO	C_PATH1	M_PATH1
Sr	cbs.gif	HD	TS_001	NO	YES	NO	C_PATH1	M_PATH1
Sr	cbs.gif	HD	TS_001	NO	YES	NO	C_PATH1	M_PATH1
Sr	cbs.gif	HD	TS_001	NO	YES	NO	C_PATH1	M_PATH1
ge	tnt.gif	HD	TS_001	NO	YES	NO	C_PATH1	M_PATH1
w	nbc.gif	HD	TS_001	NO	YES	NO	C_PATH1	M_PATH1
Smith Telephor		HD	TS_001	NO	YES	NO	C_PATH1	M_PATH1
ge	cnn.gif	HD	TS_001	NO	YES	NO	C_PATH1	M_PATH1
Sr	msnbc.gif	HD	TS_001	NO	YES	NO	C_PATH1	M_PATH1
Sr	cbs.gif	SD	TS_002	NO	YES	NO	C_PATH2	M_PATH1
Sr	cbs.gif	SD	TS_002	NO	YES	NO	C_PATH2	M_PATH1
Sr	cbs.gif	SD	TS_002	NO	YES	NO	C_PATH2	M_PATH1
Sr	cbs.gif	SD	TS_002	NO	YES	NO	C_PATH2	M_PATH1
w	nbc.gif	SD	TS_002	NO	YES	NO	C_PATH2	M_PATH1
ge	cnn.gif	SD	TS_002	NO	YES	NO	C_PATH2	M_PATH1

Services worksheet (part 2)

Table 3-5, below, describes the worksheet contents:

Table 3-5: Services worksheet contents

Column	Description
**	Two asterisks (**), with no spaces, are positioned in the first column to indicate rows to be ignored, such as rows containing column headers, or intended for future use.[1]
ID	The unique indentifier for the service. This ID is used to reference the service within and between spreadsheets. Mandatory.
TYPE	Must be STB.
ENABLE	Type YES to enable a service, NO to disable it for troubleshooting or maintenance. The corresponding **Channel Selector** button will then be hidden (i.e. replaced with an unlabeled unavailable button).

Table 3-5: Services worksheet contents (*Continued*)

Column	Description
CH NUMBER	The channel number associated with the service. Used by the GC-100 service and in the remote control area for tuning set-top boxes to this channel.
SHORT NAME	The short name of the service (e.g. call letters). Will be displayed as a heading above the thumbnail showing video from this service in the **Multi-Channel Monitoring** view, on Channel Selector buttons, and in logs of DVR recordings (see "Channel Selector" in the "Web Monitoring" chapter of the *iControl Edge Operator's Overview*. Optional. On a typical system, the **Channel Selector** buttons can fit approximately 8 characters. Longer names may appear truncated.
LONG NAME	The full name of the service. Will be displayed as a title, in the **Detailed Signal Analysis** view, and as a tooltip when the pointer is over a **Channel Selector** button. The long name also appears along with the channel number in the DVR recording area. Optional.
DESCRIPTION	Description of the service that appears in the message box at the top left of the **Detailed Signal Analysis** view. Format the text by enclosing it between valid HTML tags. Optional
LOGO FILE NAME	The name of the file containing the logo associated with this service. If present, this logo will appear at the top of the corresponding player in the **Multi-Channel Monitoring** area or **Detailed Signal Analysis** view.
LOGICAL GROUP	Organize the **Channel Selector** area, by creating logical groups of related services identified by a meaningful name. The logical group name is displayed at the bottom of the **Channel Selector** area, under the associated service buttons. The current version of iControl Edge support a maximum of 25 groups.
ALTERNATE GROUP ID	Define another set of logical groups to organize the **Channel Selector** area to suit your monitoring purposes. A meaningful name for the alternative grouping can be specified in the *Config* worksheet (see "Config Worksheet", on page 103). The current version of iControl Edge support a maximum of 25 groups.
OFFLINE	Type YES to designate a service as offline. The service will appear on the monitoring application Web pages, but will not contribute to overall alarms.
RECORDABLE	Type YES to designate a service you wish to record for a certain amount of time when an error condition is detected. The recording duration (60 seconds by default) is a configurable attribute of the DVR device specified in the manual path for this service (see "Devices Worksheet", on page 86).
EMAIL NOTIFICATION	Type YES to enable overall alarm e-mail notification on a *per service* basis. Type NO to disable it.
CYCLING PATH ID	ID of the cycling path associated with a service. This ID determines which cycling set-top box (or DVR) and which Densité probe (or pair of probes) process signals for this service.
MANUAL PATH D	ID of the manual path associated with a service. This ID determines which manual set-top box or DVR, and which streamer (if any) process signals for this service.

1. Rows you wish to leave empty must include the two asterisks in this column.

IMPORTANT: Do not change the default value for *TYPE* (STB), *ENABLED* (YES), or *OFFLINE* (NO).

To define the services at this location

1. Click the **Services** tab.
2. For each service, specify a unique ID, the associated channel number, a short name, and a long name.

   Note: The short names appear on the **Channel Selector** buttons. On a typical system, the **Channel Selector** buttons can fit approximately 8 characters. Longer names may appear truncated.

3. Insert a description (using HTML tags where appropriate), and specify the logo file name.
4. Specify a cycling path and a manual path for this service, and identify a recordable service, as required, by typing `YES` in the *RECORDABLE* column.

   Notes

   - Custom logo files can be uploaded to the following location on the Application Server:

     `/var/tomcat4/webapps/icw/sites/EDGE/images/Logo`

   - The logo images provided with the package are 52 pixels wide × 32 pixels high, but other dimensions up to 104 pixels × 64 pixels are also supported.
   - A 13:8 ratio will best fit the space available for the logos in the iControl Edge user interface.

5. Adjust the positioning of the **Channel Selector** buttons by changing the LOGICAL GROUP value.
6. Define an alternative grouping of the **Channel Selector** buttons by typing the desired group names under ALTERNATE GROUP ID.
7. For each service, specify if e-mail notification of service overall status is required (`YES`, `NO`).

Alarms Worksheet

iControl Edge shows current alarm statuses in different ways: in the **Channel Selector** area, the color of a **Channel Selector** button represents the corresponding service's overall alarm status; the alarm panel for a service displays more detailed alarm status information.

The *Alarms* worksheet defines which alarms will be monitored by your system.

	A	B	C	D	E	F	G
1	ALARMS						
2	**	DEVICE TYPE	ALARM GROUP	ALARM URI	ALARM NAME	ALARM TYPE	LEVEL
3		ACP1721	Audio	{baseuri}aChan1_ovld_ST	Ch. 1/2 Silence	COMPRESSED	SERVICE
4		ACP1721	Audio	{baseuri}aChan1_sil_ST	Ch. 1/2 Silence	COMPRESSED	SERVICE
5		ACP1721	Audio	{baseuri}aChan2_ovld_ST	Ch. 1/2 Overload	COMPRESSED	SERVICE
6		ACP1721	Audio	{baseuri}aChan2_sil_ST	Ch. 1/2 Overload	COMPRESSED	SERVICE
7		ACP1721	Audio	{baseuri}almbalance_ST	Imbalance	STATUS	SERVICE
8		ACP1721	Audio	{baseuri}aPhase_ST	Phase	STATUS	SERVICE
9	**						
10		VCP1021	Video	{baseuri}vBlackDet_ST	Black	STATUS	SERVICE
11		VCP1021	Video	{baseuri}vFreezeDet_ST	Freeze	STATUS	SERVICE
19		DEC1002	Video	{baseuri}vBlackDet_ST	Black	STATUS	SERVICE
20		DEC1002	Video	{baseuri}vFreezeDet_ST	Freeze	STATUS	SERVICE
21	**						
22		UAP1781	Audio	{baseuri}aNoSigCh1	Ch. 1/2 Silence	COMPRESSED	SERVICE
23		UAP1781	Audio	{baseuri}aNoSigCh2	Ch. 1/2 Silence	COMPRESSED	SERVICE
24	**						
25		DENSITE	Health	{baseuri}dCPUStatus	CPU Critical Load	STATUS	DEVICE
26		DENSITE	Health	{baseuri}dFan1Status	Left Fan	STATUS	DEVICE
27		DENSITE	Health	{baseuri}dPs1Status	Left Power Supply	STATUS	DEVICE
28		DENSITE	Health	{baseuri}dFanPs1Status	Left Power Supply Fan	STATUS	DEVICE
38		AS	CPU	{baseuri}CPUUser	CPU User %	TEXT	DEVICE
39		AS	Health	{baseuri}commStatus	Communication Status	STATUS	DEVICE
40		AS	Health	{baseuri}powerCycle	Device Reboot	STATUS	DEVICE
41	**						
42		HCP1801	Video	{baseuri}vBlackDet1_ST	Zone 1 Black	STATUS	SERVICE
43		HCP1801	Video	{baseuri}vFreezeDet1_ST	Zone 1 Freeze	STATUS	SERVICE

Table 3-6, below, describes the worksheet contents:

Table 3-6: Alarms worksheet contents

Column	Description
**	Two asterisks (**), with no spaces, are positioned in the first column to indicate rows to be ignored, such as rows containing column headers, or intended for future use.[1]
DEVICE TYPE	The device type to which this alarm applies: • `DENSITE` = Densité 3 Housing Frame • `AS` = Application Server • `ACP1721` = ACP-1721 Digital Audio Control Probe • `VCP1021` = VCP-1021 Composite Control Probe • `DEC1002` = DEC-1002 10-Bit Composite to SDI Decoder • `DEC1003` = DEC-1003 10-Bit Composite to SDI Decoder with Probing Option • `DEC1023` = DEC-1023 12-Bit 3D Composite to SDI Decoder with Probing • `UAP1781` = UAP-1781 8-Channel Universal Audio Processor • `UAP1783` = UAP-1783 8-Channel Universal Audio Processor • `AAP1741` = AAP-1741 4-Channel Analog Audio Processor • `HCP1801` = HCP-1801 HD/SD Video Control Probe with Embedded Audio
ALARM GROUP	The group to which this alarm belongs. Will be displayed as a header in the alarm panel.
ALARM URI	The alarm's Uniform Resource Identifier.
ALARM NAME	The name of the alarm that appears in the **Detailed Signal Analysis** views (see the *Alarm Browser* section in the *Web Monitoring* chapter of the *iControl Edge Operator's Overview*).

Table 3-6: Alarms worksheet contents (*Continued*)

Column	Description
ALARM TYPE	The type of alarms (TEXT, STATUS).
LEVEL	Specifies whether the alarm belongs to the Device or Service category. An alarm set to the SERVICE level is visible in the service's alarm panel, and its state contributes to the overall alarm status for this service. The service's button color in the **Channel Selector** area represents this overall alarm status. An alarm set to the DEVICE level is also visible in the service's alarm panel, but its state does not contribute to the alarm status for this service (and thus does not affect the color of the corresponding **Channel Selector** button).

1. Rows you wish to leave empty must include the two asterisks in this column.

To define the alarms covered by your iControl Edge configuration

1. Click the **Alarms** tab.
2. If desired, change the *ALARM NAME*—this will change the text displayed in the monitoring application.

IMPORTANT: Do not change the value for *ALARM URI*.

Note: If you wish to discontinue monitoring for a specific alarm, insert two asterisks (**) in the first column of the corresponding row, or delete the entire row. The alarm will be removed from all Alarm Panels and will no longer be calculated or displayed.

Config Worksheet

The *Config* worksheet defines alarm behavior, and other options.

CONFIG			
**	KEY	VALUE	COMMENT
	blinkWhenUnacknowledged	NO	
	ackAudibleAlarm	YES	Show audible mute/acknowledge buttons
	alternateGroupLabel	TS	Grouped by transport stream
**	EMBEDDED WEB PAGES (setting a value will enable a button in the Application Browser)		
	browserButton0_url	http://www.miranda.com	URL to load
	browserButton0_title	Miranda	Button text
	browserButton0_image	../Images/Links/ie_unselected.gif	Button image (URL or relative to EDGE/Web_pages)
	browserButton0_selectedImage	../Images/Links/ie_selected.gif	Selected button image (URL or relative to EDGE/Web_pages)
**			
**	browserButton1_url	google.com	URL to load
**	browserButton1_title	Google	Button text
**	browserButton1_image		Button image (URL or relative to EDGE/Web_pages)
**	browserButton1_selectedImage		Selected button image (URL or relative to EDGE/Web_pages)
**	EMAIL NOTIFICATION		
**	smtpServer	ca-ops-mail	The SMTP server ip adress or hostname
**	smtpUsername		Optionally if authentication is required with the SMTP server
**	smtpPassword		Optionally if authentication is required with the SMTP server
**	emailRecipient	ktarhini@miranda.com	recipient e-mail addresses (comma separated)
**	emailSender	gsm@miranda.com	Sender email adress
**	emailSubject	Miranda EDGE alarm notification	The email subject

Table 3-7, below, describes the worksheet contents:

Table 3-7: Config worksheet contents

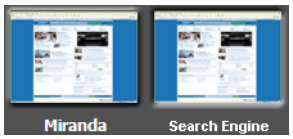
Key	Description
blinkWhenUnacknowledged	Default value is NO. Setting this value to YES causes new alarms to blink in the monitoring application page. Operator has to acknowledge individual alarms to stop the blinking. If ackAudibleAlarm is enabled, the operator can click **Acknowledge** to acknowledge all alarms at once.
ackAudibleAlarm	Default YES value causes an audible alarm (chime) to activate when a new alarm comes in, and allows operators to temporarily mute the chime, by clicking **Acknowledge**. When another alarm comes in, the audible alarm will be re-activated. Click **Mute** to mute the audible alarm and prevent it from being re-activated automatically (until you decide otherwise by clicking **Unmute sound**). Set ackAudibleAlarm to NO to disable the audible alarm, and hide both the **Acknowledge** and **Mute**/**Unmute** sound buttons.
alternateGroupLabel	The **Channel Selector** can be sorted on the basis of some criteria, including logical groups defined in the *Services* worksheet and referred to as Logical group in the context of the **Channel Selector**'s sort menu. The alternate label you can provide here will appear in the **Channel Selector**'s sort menu to designate an additional set of groups, also defined in the *Services* worksheet (see "Services Worksheet", on page 99). Default value is TS (i.e. *transport stream*).
--- EMBEDDED WEB PAGES ---	
In the **Embedded Web Pages** area, you can define and configure up to two custom Application Selector buttons linked to Web pages or iC Web pages. To configure a button, remove the asterisks at the beginning of the corresponding rows (the set of four rows that start with either browserButton0 or browserButton1), and type the desired values for the four parameters (the parameters for the first button are described below; the other button is configured in the same fashion). A custom button is added to the application Selector, only if the associated URL or MPF file path is specified. 	
browserButton0_url	The address of a Web page (URL) or iC Web page (path to MPF file, relative to EDGE/Web_pages). For example: http://www.miranda.com.
browserButton0_title	The label of the button (Miranda by default).
browserButton0_image	**Unselected** button image (URL, or path to image file, relative to EDGE/Web_pages).
browserButton0_selectedImage	**Selected** button image (URL, or path to image file, relative to EDGE/Web_pages).
--- EMAIL NOTIFICATION ---	
In the **E-mail Notification** area, you can identify the outgoing SMTP mail server and e-mail recipients of overall service alarm notifications.	
smtpServer	The DNS of the mail server. Mandatory when e-mail notification is enabled.

Table 3-7: Config worksheet contents (*Continued*)

Key	Description
smtpUsername	The sending user's e-mail user ID. Optional.
smtpPassword	The sending user's e-mail password. Optional.
emailRecipient	The recipient user's e-mail address. Mandatory when e-mail notification is enabled.
emailSender	The sending user's e-mail address. Optional.
emailSubject	The desired Subject line of the e-mail. Optional.

To define the alarm behavior and other options for your iControl Edge configuration

- Click the **Config** tab, and specify the appropriate values for the attributes described in Table 3-7, above.

> **Note:** Remember to save all changes to the *Config* worksheet once you have finished.

[Special Case] Spreadsheet Inheritance

Typically, the topology of an iControl Edge setup is diffuse in nature, with multiple Application Servers serving as hubs, each to their own set of Densité probes and cyclers. In the past, this necessitated manually defining all channels at each location. The Spreadsheet Inheritance feature allows a single Application Server to manage the devices and services of multiple locations.

Configuring Spreadsheet Inheritance

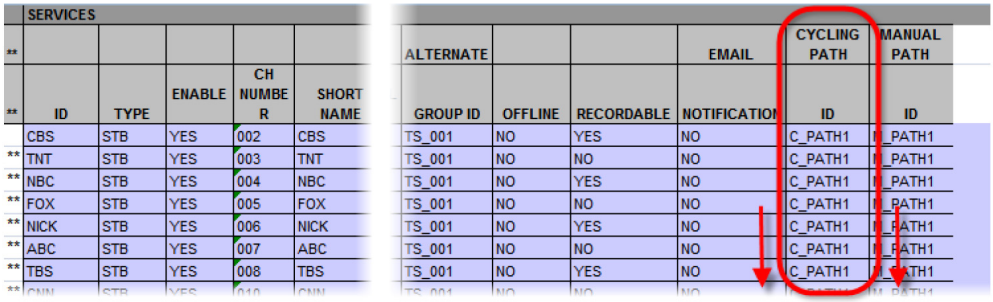
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have downloaded the `Locations.xls` spreadsheet from the intended head-end Application Server (see "Downloading the iControl Edge Configuration Spreadsheets", on page 82)
- If you intend on managing Densité services of one or more hub Application Servers from the head-end, you have downloaded the configuration spreadsheets from the head-end Application Server.
- You have, on hand, the IP address, host name, and ID of your intended head-end Application Server.

To configure spreadsheet inheritance

1. In the `Locations.xls` spreadsheet of your head-end Application Server, click the **Locations** tab.
2. In the *IP* column for all rows, type the IP address corresponding to the intended master Application Server.
3. In the *HOSTNAME* column for all rows, type the host name corresponding to the intended master Application Server.
4. Click the *Services* tab.
5. Take note of all the cycling paths in the *CYCLING PATH ID* column.



	SERVICES											
**						ALTERNATE			EMAIL	CYCLING PATH	MANUAL PATH	
**	ID	TYPE	ENABLE	CH NUMBER	SHORT NAME	GROUP ID	OFFLINE	RECORDABLE	NOTIFICATION	ID	ID	
	CBS	STB	YES	002	CBS	TS_001	NO	YES	NO	C_PATH1	M_PATH1	
**	TNT	STB	YES	003	TNT	TS_001	NO	NO	NO	C_PATH1	M_PATH1	
**	NBC	STB	YES	004	NBC	TS_001	NO	YES	NO	C_PATH1	M_PATH1	
**	FOX	STB	YES	005	FOX	TS_001	NO	NO	NO	C_PATH1	M_PATH1	
**	NICK	STB	YES	006	NICK	TS_001	NO	YES	NO	C_PATH1	M_PATH1	
**	ABC	STB	YES	007	ABC	TS_001	NO	NO	NO	C_PATH1	M_PATH1	
**	TBS	STB	YES	008	TBS	TS_001	NO	YES	NO	C_PATH1	M_PATH1	

6. Click the *Paths* tab.
7. Define all cycling paths you noted in step 5:
   a) In the *ID* column, type the *CYCLING PATH ID* value from the *Services* tab.
   b) In the *TYPE* column, type `STB_CYCLING`.
   c) In the *ENABLE* column, type `YES`.

PATHS			
**			
**	ID	TYPE	ENABLE
	C_PATH1	STB_CYCLING	YES
	C_PATH2	STB_CYCLING	YES
	C_PATH3	STB_CYCLING	YES
	C_PATH4	STB_CYCLING	YES
	C_PATH5	STB_CYCLING	YES
**			
**	ID	TYPE	ENABLE
	M_PATH1	STB_MANUAL	YES

8. Click the *Config* tab.
9. In the *KEY* column, type `inheritance`.
10. In the *VALUE* column, type `YES`.

CONFIG			
**	KEY	VALUE	COMMENT
	inheritance	YES	

11. Save the spreadsheet and upload it to the head-end Application Server (see page 110).
12. Perform the following sub-steps for each instance of Densité Manager you would like to manage from your head-end Application Server:
    a) Open the *Configuration* spreadsheet of the hub Application Server.
    b) Click the *Devices* tab.
    c) In the *APPLICATION SERVER* section, in a new row, type the following information corresponding to the head-end Application Server:
    - *ID*: `<Application Server ID>`
    - *TYPE*: `AS`
    - *ENABLE*: `YES`
    - *IP*: `<IP address of head-end>`
    - *HOSTNAME*: `<host name of head-end>`

    d) In the *DENSITE* section, locate the Densité you would like to manage on the head-end, and then type the ID of the head-end Application Server in the *APP SERVER ID* column.
    e) Save the spreadsheet.

f) Upload the spreadsheet to the head-end Application Server (see page 110).

13. Restart the head-end Application Server.

Confirming Inheritance Configuration is Successful

REQUIREMENT

Before beginning this procedure, make sure you have opened iControl Edge (see "Launching the iControl Edge Web Site", on page 112).

To confirm you have successfully configured inheritance

1. In iControl Edge, click the **APPS** tab in the **Application Browser** area.

   The **Application Selector** appears.

2. Click **Alarm Browser**.

   The GSM Alarm Browser appears.

3. In the Alarm Browser's left pane, click any one of the hub Application Servers **EXCEPT** the head-end.

4. On the right pane, verify that there are no cyclers, virtual alarms, or GC-100 service. If there are, you did not successfully configure spreadsheet inheritance.

5. On the right pane, expand the **iControl** sub-folder.

   If you configured the Densité Manager to be on the head-end, the only alarms you should see listed in this folder are physical alarms for the Densité probes belonging to this hub. If you see any virtual alarms, you have not successfully configured spreadsheet inheritance. Only the master should have virtual alarms, cyclers, and GC-100 alarms in the **iControl** sub-folder.

Task 12: Uploading and Applying iControl Edge Configuration Files

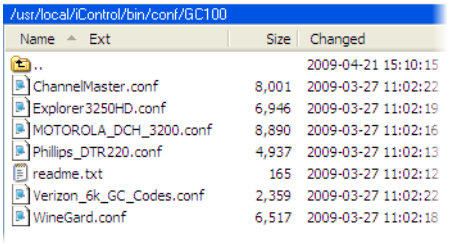
Once you have finished modifying the configuration spreadsheets, and creating the required configuration files for the Global Caché GC-100 Network Adapter, you must transfer them to the Application Server and restart the GSM services (see "Restarting the General Status Manager (GSM) Services", on page 111) for the changes to take effect.

Uploading the GC-100 Network Adapter Configuration Files

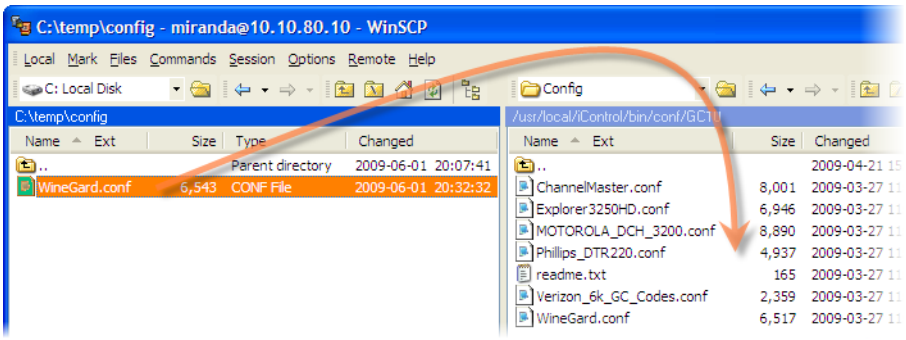
You can use any suitable file transfer application—WinSCP, for instance, or the upload function of the Application Server's File Manager utility—to transfer new or updated configuration files from your client PC or laptop to the Application Server.

To upload the configuration files to the Application Server

1. Launch WinSCP, log on to the Application Server and navigate to `/usr/local/iControl/bin/conf/GC100`.



2. Select the new or modified configuration files (`.conf`) on your PC or laptop, and then drag them to the GC100 directory on the Application Server.



3. Close WinSCP.

   You have successfully uploaded the configuration files for your GC-100 Network Adapter.

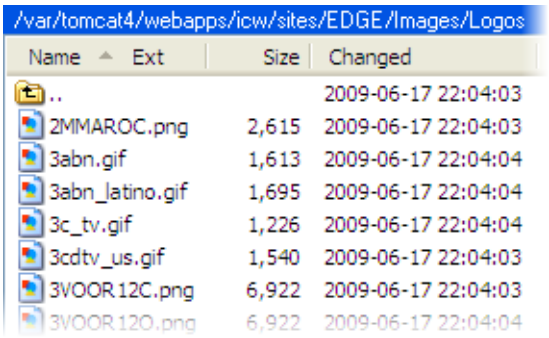
Uploading Custom Logo Files

Your iControl Edge system ships with a set of predefined logo files located under `/var/tomcat4/webapps/icw/sites/EDGE/images/Logo` on the Application Server. You can add custom logo files to this directory.

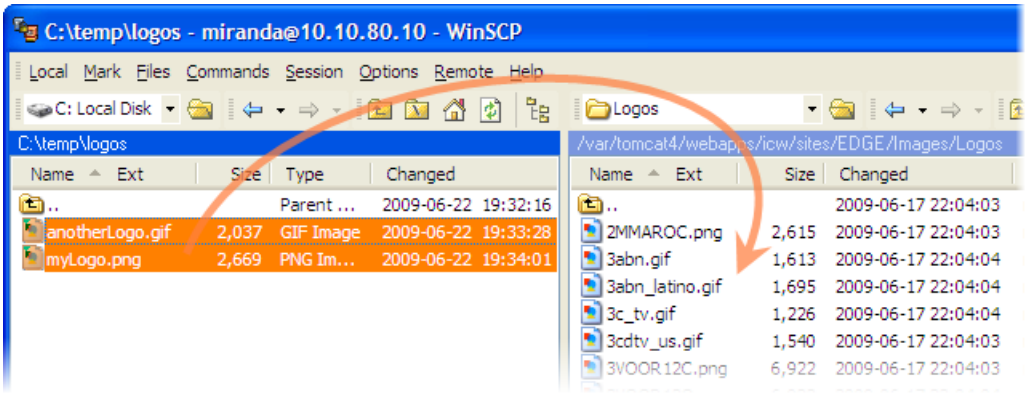
> **Note:** When you update your system with a new version of the iControl Edge package, any existing logo file that is not part of the default logo set, or that is more recent than a logo file with the same name within the default set, will be carried forward. Nevertheless, it is always advisable to keep a backup copy of your custom logo files (e.g. on your hard drive).

To upload custom logo files to the Application Server

1. Launch WinSCP, log on to the Application Server and navigate to: `/var/tomcat4/webapps/icw/sites/EDGE/images/Logo`.



2. Select the custom logo files (GIF or PNG) on your PC or laptop, and then drag them to the Logos directory on the Application Server.


C:\temp\logos - miranda@10.10.80.10 - WinSCP
Local Mark Files Commands Session Options Remote Help
C: Local Disk
Logos
C:\temp\logos
/var/tomcat4/webapps/icw/sites/EDGE/Images/Logos
Name Ext Size Type Changed
.. Parent ... 2009-06-22 19:32:16
anotherLogo.gif 2,037 GIF Image 2009-06-22 19:33:28
myLogo.png 2,669 PNG Im... 2009-06-22 19:34:01
Name Ext Size Changed
.. 2009-06-17 22:04:03
2MMAROC.png 2,615 2009-06-17 22:04:03
3abn.gif 1,613 2009-06-17 22:04:04
3abn_latino.gif 1,695 2009-06-17 22:04:04
3c_tv.gif 1,226 2009-06-17 22:04:04
3cdtv_us.gif 1,540 2009-06-17 22:04:03
3VOOR12C.png 6,922 2009-06-17 22:04:03

3. Close WinSCP.

See also

For more information about logo files, see "Services Worksheet", on page 99.

Uploading the iControl Edge Configuration Spreadsheets

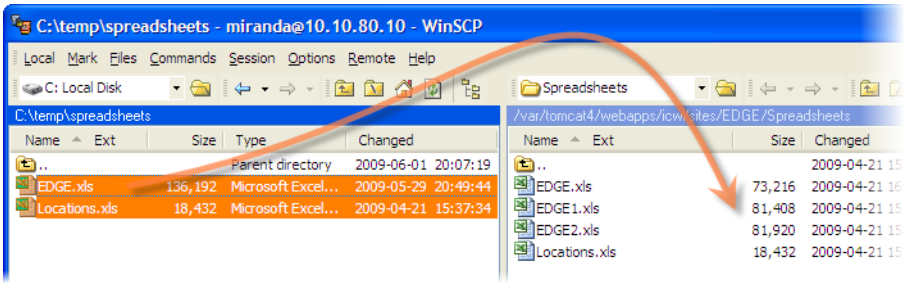
You can use any suitable file transfer application—WinSCP, for instance, or the upload function of the Application Server's File Manager utility—to transfer updated spreadsheets from your client PC or laptop back to the Application Server.

To upload the configuration spreadsheets to the Application Server

1. Launch WinSCP, log on to the Application Server and navigate to:
   `/var/tomcat4/webapps/icw/sites/EDGE/Spreadsheets/`

   See "Downloading the iControl Edge Configuration Spreadsheets", on page 82.

2. Select the modified spreadsheet (`.xls`) files on your PC or laptop, and then drag them to the Spreadsheets directory on the Application Server.



3. Close WinSCP.

   You have successfully uploaded your modified configuration spreadsheets.

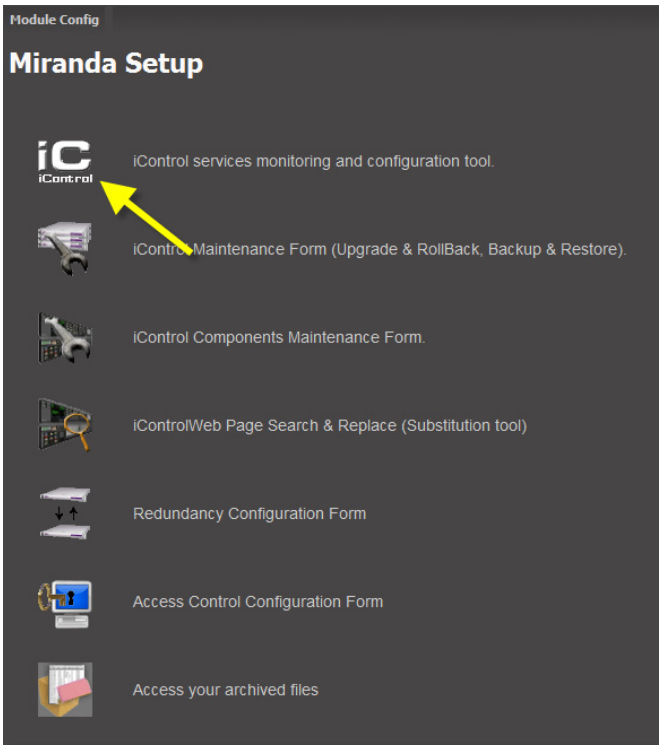
Restarting the General Status Manager (GSM) Services

Once you have uploaded the modified iControl Edge Configuration Spreadsheets, you must restart iControl's General Status Manager (GSM) services, and refresh the iControl Edge Web page for the changes to take effect.

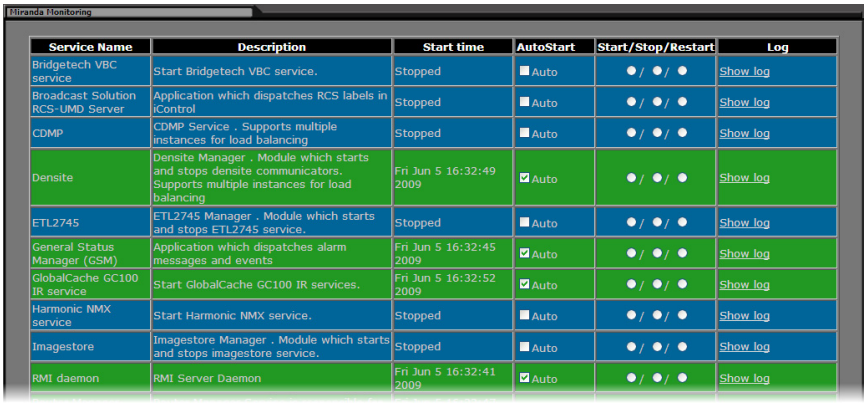
To restart iControl's GSM services

1. Log on to Webmin (see "Logging on to Webmin", on page 30).
2. Click **Miranda iControl Management Tool**.

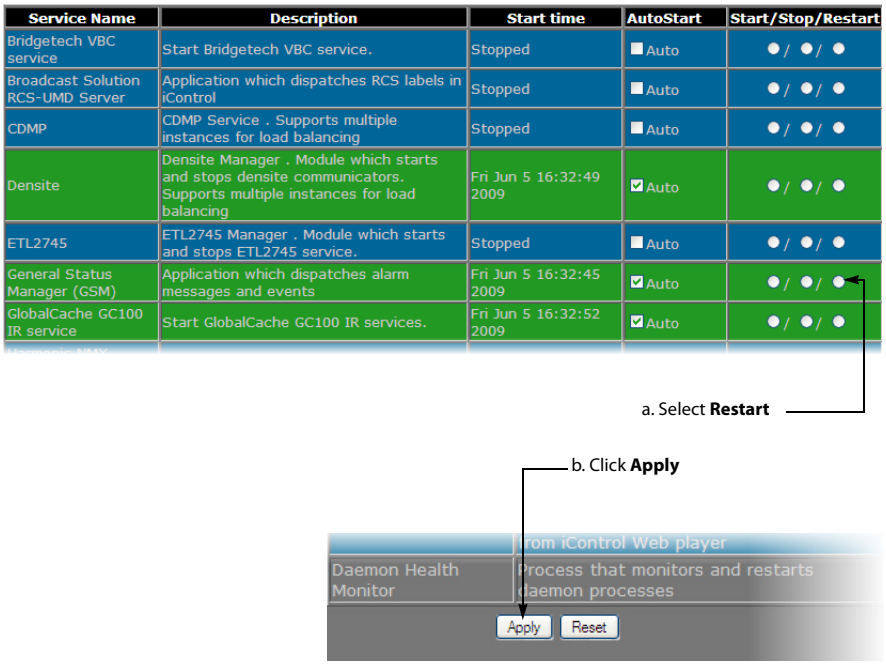
   The Miranda Setup page appears.
3. Click the iControl logo next to **iControl services monitoring and configuration tool**.


Module Config
Miranda Setup
iControl services monitoring and configuration tool.
iControl Maintenance Form (Upgrade & RollBack, Backup & Restore).
iControl Components Maintenance Form.
iControlWeb Page Search & Replace (Substitution tool)
Redundancy Configuration Form
Access Control Configuration Form
Access your archived files

The Miranda Monitoring page appears.



4. In the **Start/Stop/Restart** column, select **Restart**, for all General Status Manager (GSM) services listed on the page, and then click **Apply** at the bottom of the page.



You have successfully restarted the GSM services and applied the settings contained in your modified Configuration Spreadsheets.

Launching the iControl Edge Web Site

The iControl Edge system is designed to be ready for operation from the moment the initial setup is completed. When the Application Server at the central monitoring location, and all remote Application Servers, Densité frames, GC-100 network adapters and Allégro systems are configured and online, an operator with network access can get started simply by launching the iControl Edge Web site.

Note: The iControl Edge Web site can be accessed from any PC or laptop on the same network as the Application Server. iControl Edge offers several pre-configured versions of its main Web page. Choose either a dual-screen or a single-screen layout, with the appropriate resolution for your client PC or laptop.

To launch the iControl Edge Web site

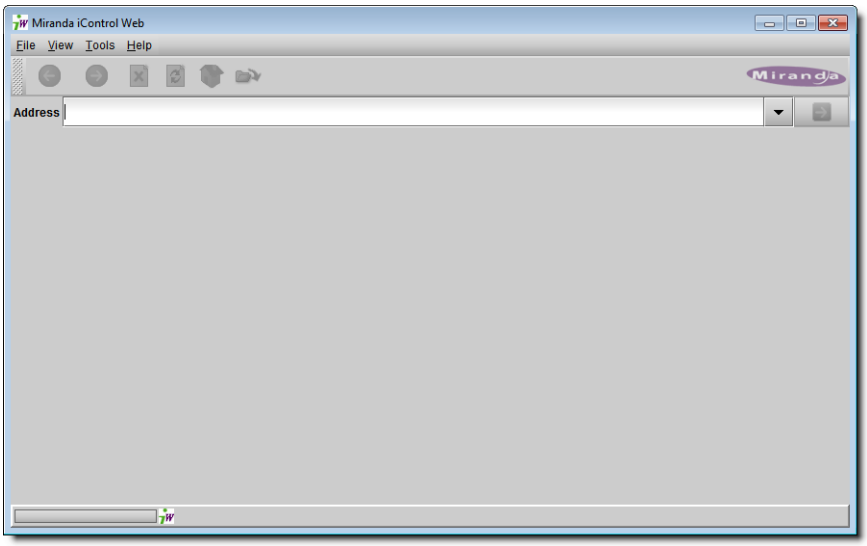
1. From a client PC or laptop on the same network as the Application Server, open a Web browser and type the Application Server's IP address in the address bar.

   The iControl Startup Page appears.

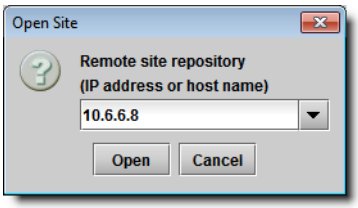
2. Click **iC Web**.

   The Java Web Start window opens, and the iControl Web application is downloaded to your PC or laptop. When the download is completed, the iControl Web splash screen appears.

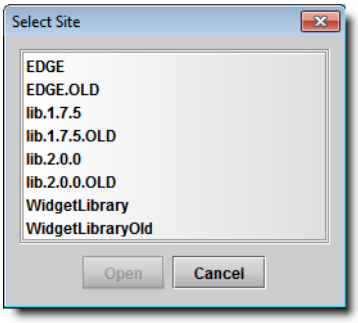
A few seconds later, the iControl Web browser window appears.



3. On the **File** menu, click **Open Site**.
4. In the **Open site** window that appears, type the Application Server's IP address.



5. In the **Select site** window, double-click **EDGE**.

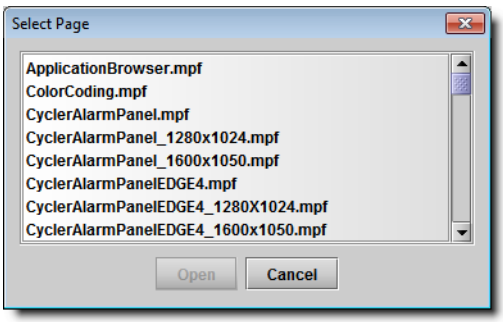


Note: You may see other versions of the EDGE Web site. These are backups of previous versions that were saved when updating the Web site, and could be useful should you need to revert to an older version.

6. In the **Select page** window, double-click the desired home page.

   For instance:

   - `Home.mpf`, if you have two 1600 × 1200 monitor
   - `HomeEDGE4.mpf`, if you have a 4-input head-end and two 1600 × 1200 monitor
   - `Home1280x1024.mpf`, for a single monitor with a resolution of 1280 × 1024
   - `Home_1600x1050x2.mpf`, if you have two 1600 × 1050 monitors in Multiple Monitor[1] mode
   - `HomeEDGE4_1600x1050x2.mpf`, if you have a 4-input head-end and two 1600 × 1050 monitors in Multiple Monitor mode



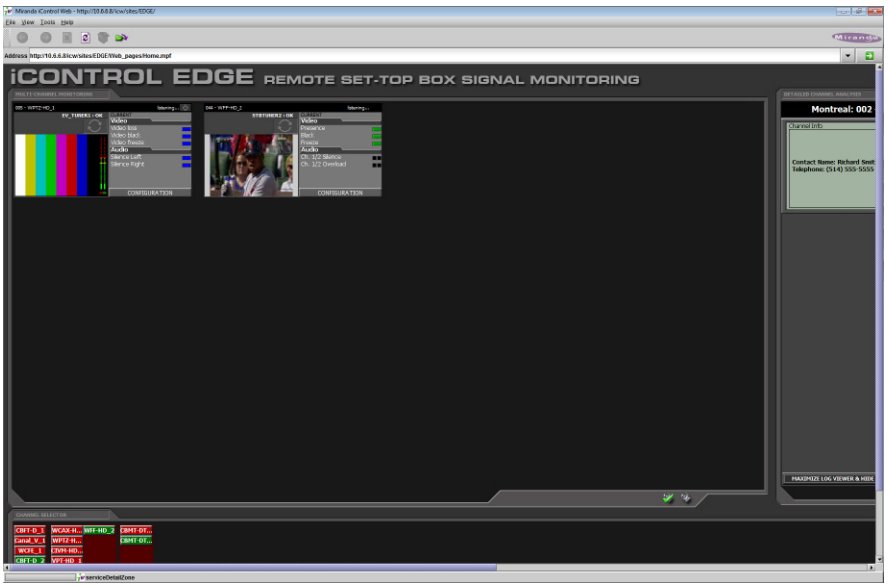
   The current version of iControl Edge includes three sets of pre-configured single-screen and double-screen home pages: one set for systems with typically 4 set-top boxes, another one for systems with 8 set-top boxes, and the default set for system with 16 set-top boxes. The table below shows the supported monitor resolutions:

1. Multiple Monitor mode is when you have two monitors connected to one PC and you expand your primary display to the second monitor.

Supported monitor resolutions

Resolution	Single / dual	16-player monitoring area	8-player monitoring area	4-player monitoring area
1280 × 1024	1 screen	Home_1280x1024	HomeEDGE8_1280x1024	HomeEDGE4_1280x1024
	2 screens	Home_1280x1024x2	HomeEDGE8_1280x1024x2	HomeEDGE4_1280x1024x2
1600 × 1050	1 screen	Home_1600x1050	HomeEDGE8_1600x1050	HomeEDGE4_1600x1050
	2 screens	Home_1600x1050x2	HomeEDGE8_1600x1050x2	HomeEDGE4_1600x1050x2
1600 × 1200	1 screen	Home_1600x1200	HomeEDGE8_1600x1200	HomeEDGE4_1600x1200
	2 screens	Home	HomeEDGE8	HomeEDGE4
1680 × 1050	1 screen	Home_1680x1050	HomeEDGE8_1680x1050	HomeEDGE4_1680x1050
	2 screens	Home_1680x1050x2	HomeEDGE8_1680x1050x2	HomeEDGE4_1680x1050x2
1920 × 1080	1 screen	Home_1920x1080	HomeEDGE8_1920x1080	HomeEDGE4_1920x1080
	2 screens	Home_1920x1080x2	HomeEDGE8_1920x1080x2	HomeEDGE4_1920x1200
1920 × 1200	1 screen	Home_1920x1200	HomeEDGE8_1920x1200	HomeEDGE4_1920x1200
	2 screens	Home_1920x1200x2	HomeEDGE8_1920x1200x2	HomeEDGE4_1920x1200x2

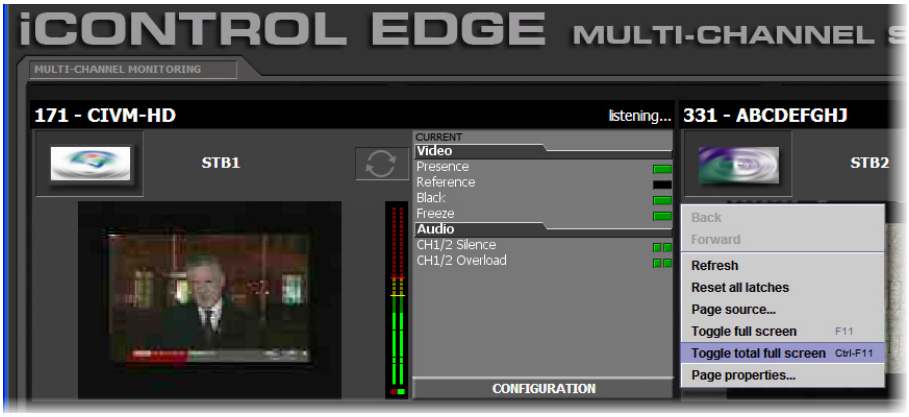
In a few moments, the iControl Edge Web interface appears.



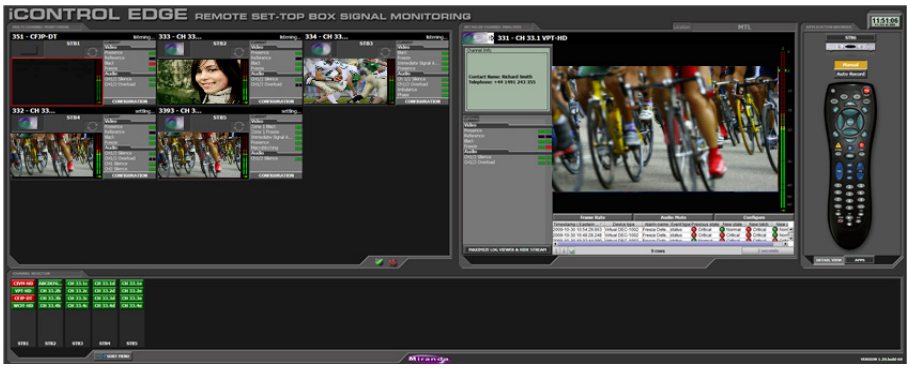
7. On the **View** menu, click **Total full screen** (or press **Ctrl**+**F11**) to display the full screen over dual monitors if you chose a dual-screen layout.
8. Click **Full screen** (or press **F11**) if you chose a single-screen layout.

> **Note:** Press **F11** or **Ctrl**+**F11** again to restore the iC Web window.

9. Alternatively, right-click in a blank area between elements on the Web page (e.g. between thumbnails, or between the banner and the monitoring area), and then click **Toggle total full screen** (or **Toggle full screen**).



The complete monitoring Web page appears in full screen mode.



iControl Edge dual-screen Web page in total full screen mode (over two monitors)

iControl Edge single-screen Web page in full screen mode.

10. If you set this site as your home page, you will not need to go through the selection steps described above any more.

> **Note:** To set this site to open by default, click **Set home page** on the **Tools** menu.

The next time you open iControl Web, this iControl Edge Web page will appear by default.

Congratulations—your iControl Edge system is now ready for operation! For a more complete description of the monitoring application, please refer to the iControl Edge Operator's Overview.

A Troubleshooting

If you encounter problems with your iControl Edgesystem, you should begin your troubleshooting by verifying that the client PC and the Application Server are networked correctly to the other devices that are part of your system.

Verifying Device Connectivity

One way of verifying that the client PC and the Application Server are networked correctly to the other devices that are part of your system is to use an SSH client such as PuTTY to ping them from the Application Server. If you do not have PuTTY installed on your PC, see "Installing PuTTY", on page 121

To verify that a device is properly connected to your system

1. Launch PuTTY and log on to the Application Server (see "Establishing an SSH Connection with an Application Server", on page 122).
2. In the PuTTY command line window, type the following:

   `ping AAA.BBB.CCC.DDD`

   where `AAA.BBB.CCC.DDD` is the IP address of a Global Caché GC-100 Network Adapter.

   A message similar to the following should appear:

   `Reply from AAA.BBB.CCC.DDD: bytes=32 time<1ms TTL=62`
3. If the `ping` command is successful, stop the ping by pressing **Ctrl**+**C**.
4. If the message does not appear within a second, stop the ping by pressing **Ctrl**+**C**, and then verify that the device is powered up, properly cabled, and that its IP address is correctly configured.
5. For each Global Caché GC-100 Network Adapter, type the following command:

   `ping AAA.BBB.CCC.DDD`

   where `AAA.BBB.CCC.DDD` is the GC-100's IP address (e.g. `192.168.1.70`).

   A message similar to the following should appear:

   `Reply from AAA.BBB.CCC.DDD: bytes=32 time<1ms TTL=62`
6. If the `ping` command is successful, stop the ping by pressing **Ctrl**+**C**.
7. If the message does not appear within a second, stop the ping by pressing **Ctrl**+**C**, and then verify that the device is powered up, properly cabled, and that its IP address is correctly configured.
8. For each Allégro system in your configuration, type the following command:

   `ping AAA.BBB.CCC.DDD`

where `AAA.BBB.CCC.DDD` is the Allégro system's IP address (e.g. `10.0.3.7`).

A message similar to the following should appear:

```
Reply from AAA.BBB.CCC.DDD: bytes=32 time<1ms TTL=62
```

9. If the `ping` command is successful, stop the ping by pressing **Ctrl**+**C**.
10. If the message does not appear within a second, stop the ping by pressing **Ctrl**+**C**, and then verify that the device is powered up, properly cabled, and that its IP address is correctly configured.
11. Type `exit`, and then press **Enter** to close the PuTTY command line window.
12. If your problem persists, consult the troubleshooting chart below.

Troubleshooting Chart

Troubleshooting actions

Symptom	Action
iControl Edge Web monitoring interface does not load	Verify that the IP addresses of the various devices that are part of your system are set correctly in the configuration spreadsheet for the selected location (see "Devices Spreadsheet", on page 86). If a device is not detected on the network, attempts to load the iControl Edge Web interface may continue for several minutes, until a communication timeout occurs.
All alarms in the Alarm Panels are blue	Verify that the GSM and Densité Manager services are active on the Application Server. See: • "Restarting the General Status Manager (GSM) Services", on page 111 • "Enabling Densité Manager Services", on page 55
No video in a player	Open the control panel for the video probe associated with the player and enable thumbnail streaming (see "Enabling Thumbnail Streaming", on page 59).
No audio at the client PC	Verify that the Audio Mute button in the monitoring page is not in the Mute position. Mute is ON any time a new stream is selected. Click **Monitor this stream** on the Allégro System Status page. When the Miranda Streaming Player window opens, check to see if the audio level meter indicates any activity. If there is no activity, then it is likely that the Allégro is not receiving audio input. On the Allégro Streaming Encoder Configuration page, verify that Audio is set to: • Enabled=Yes • MAC2- 44100 samp./sec • 16 bit stereo
No video at the client PC	Verify that the RCA composite video input cable is connected to port 1 (right-hand side) of the video capture card on the back of the Allégro. Verify that the video encoder is running on the Allégro Streaming Encoder Status page (from the Allégro Web interface, under **Streaming Encoder** in the left navigation bar, click **Status**).

B Installing PuTTY

PuTTY is an open-source terminal emulator application that supports the SSH protocol. It can be used to establish an SSH connection with Miranda Application Servers.

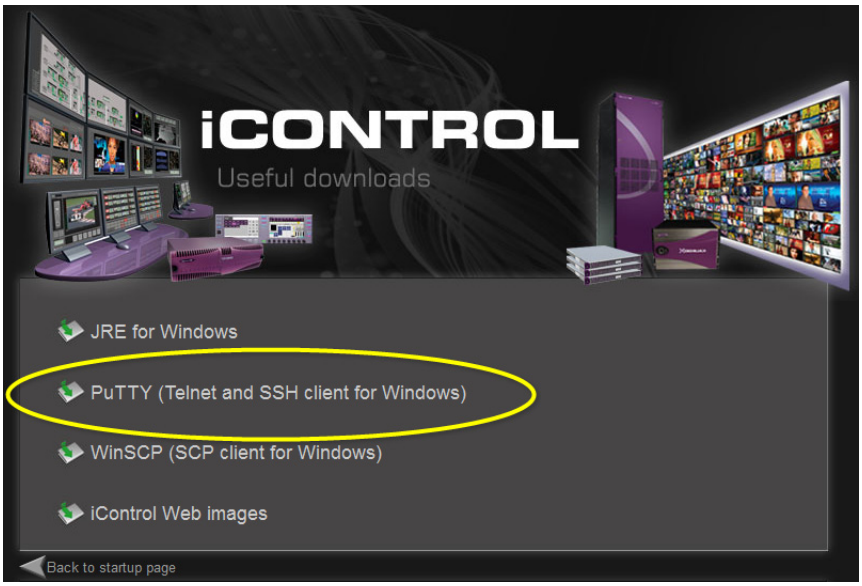
Installing PuTTY

PuTTY is available from your Application Server's Useful Downloads page.

To install PuTTY on your client PC or laptop

1. Open an Application Server's Startup Page in a Web browser.
2. On the iControl Startup page, click **Useful Downloads**.

3. On the Useful Downloads page, click **PuTTY** to download the PuTTY executable file (`putty.exe`).



4. When prompted, save the file to your desktop, or some other location on your PC or laptop.

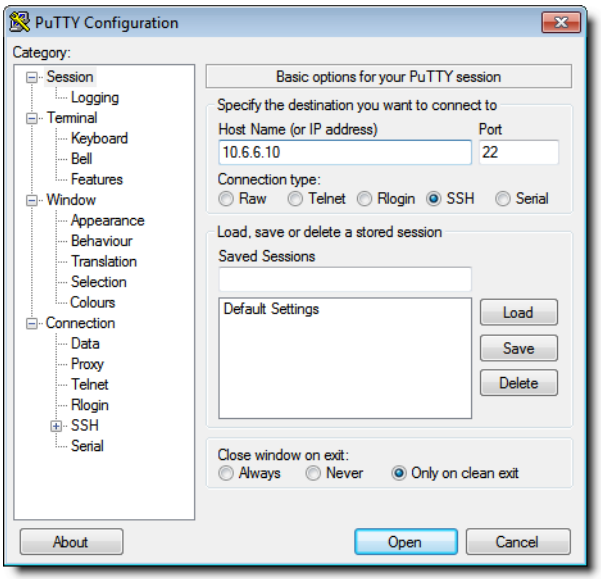
Establishing an SSH Connection with an Application Server

To establish an SSH connection with the Application Server

1. Browse to the PuTTY executable file on your PC or laptop, and then open it.

> **Note:** If Windows prompt you about the application's signature, click **Yes**.

The PuTTY Configuration window appears.



2. In the **Session** panel, specify your Application Server's IP address or host name, make sure that SSH is the selected connection type, and then click Open.

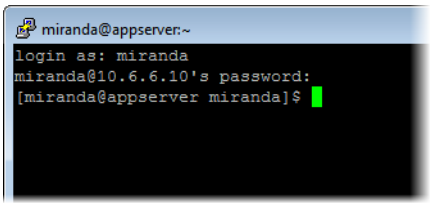
   Note: If the **PuTTY Security Alert** window appears, click **Yes** to close it.

   A command line window appears, prompting you for a user name.

   Note: Application Servers are configured by default with the user name `miranda` and the password `icontrol`, but these may have been changed by your system administrator.

3. Type `miranda`, and then press **Enter**.
4. When prompted for a password, type `icontrol`, and then press **Enter**.

   You are now connected to the Application Server.



Ending a PuTTY Session

To end the SSH session

- Type `exit`, and then press **Enter** to close the PuTTY command line window.

C Using WinSCP

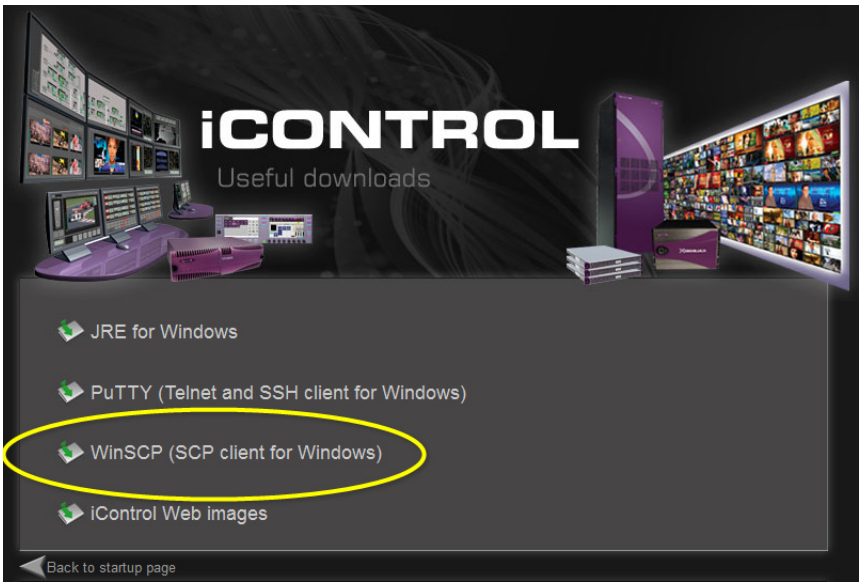
WinSCP (Windows Secure copy) is an open source SFTP and FTP client for Microsoft Windows. Its main function is secure file transfer between a local and a remote computer. It can be used (in place of the Webmin File Manager) to copy files to and from Application Servers.

Installing WinSCP

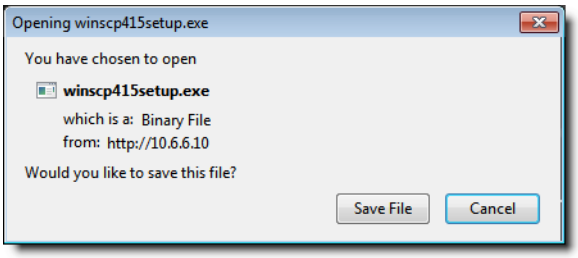
To install WinSCP on your PC

1. Open an Application Server's Startup page in a Web browser.
2. Click **Useful downloads**.

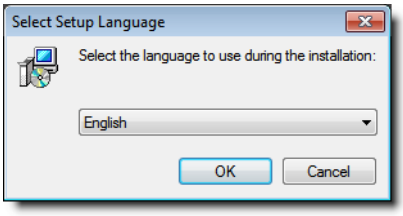
3. Click **WinSCP**.



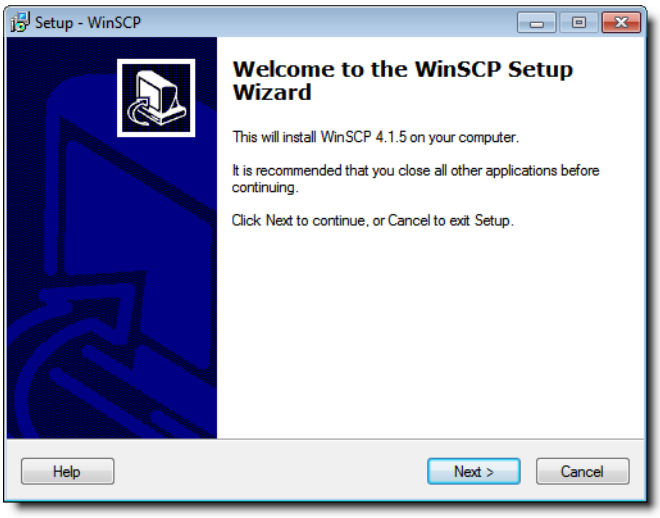
4. When prompted, click **Save File** to save the WinSCP installer to your PC.



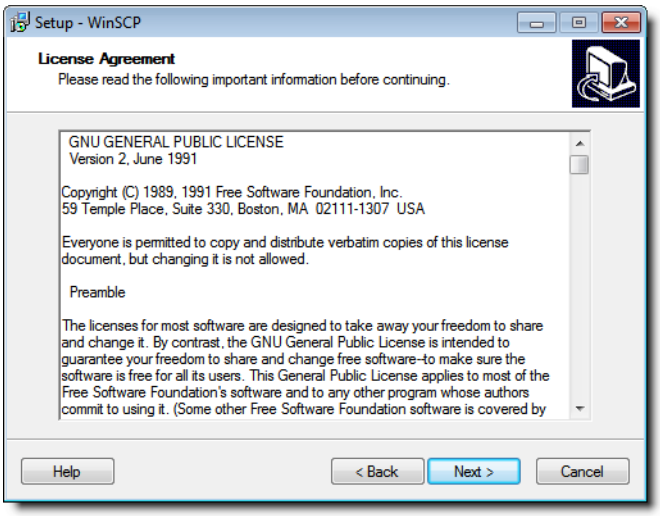
5. When the download is complete, open the executable file. If a security warning appears, click **Run**.
6. When prompted, select a language, and then click **OK**.



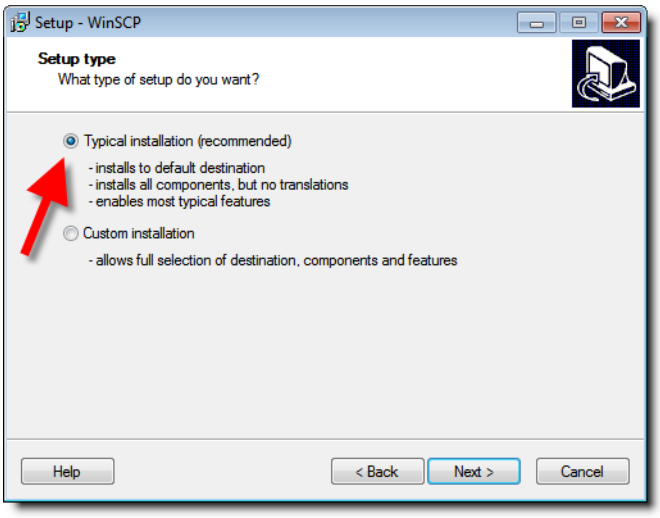
7. When the WinSCP Setup Wizard appears, click **Next**.


Setup - WinSCP
Welcome to the WinSCP Setup Wizard
This will install WinSCP 4.1.5 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Help
Next >
Cancel

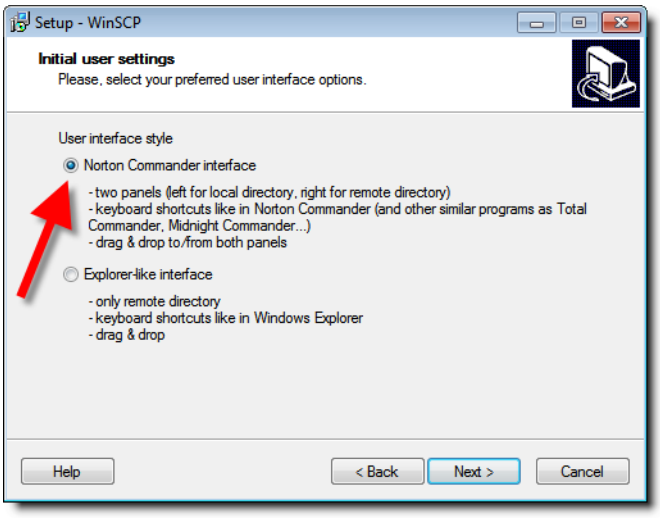
8. When the License Agreement appears, click **Next**.


Setup - WinSCP
License Agreement
Please read the following important information before continuing.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by
Help
< Back
Next >
Cancel

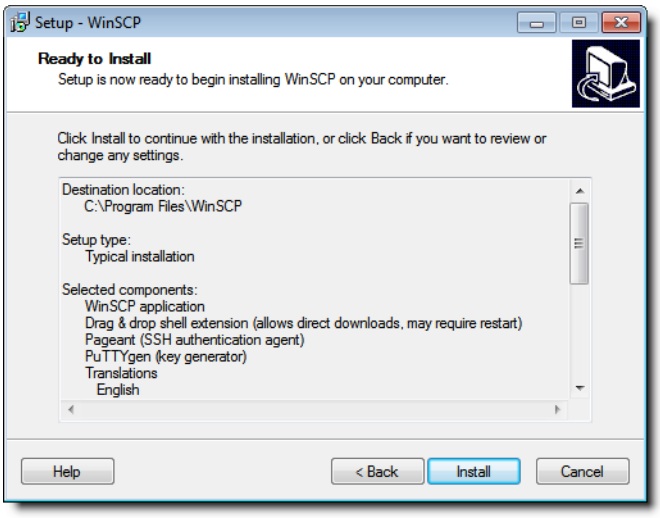
9. In the **Setup type** window, select **Typical installation**, and then click **Next**.


Setup - WinSCP
Setup type
What type of setup do you want?
Typical installation (recommended)
- installs to default destination
- installs all components, but no translations
- enables most typical features
Custom installation
- allows full selection of destination, components and features
Help
< Back
Next >
Cancel

10. When the Initial user settings window appears, select **Norton Commander interface**, and then click **Next**.


Setup - WinSCP
Initial user settings
Please, select your preferred user interface options.
User interface style
Norton Commander interface
- two panels (left for local directory, right for remote directory)
- keyboard shortcuts like in Norton Commander (and other similar programs as Total Commander, Midnight Commander...)
- drag & drop to/from both panels
Explorer-like interface
- only remote directory
- keyboard shortcuts like in Windows Explorer
- drag & drop
Help
< Back
Next >
Cancel

11. When the **Ready to install** window appears, click **Install** to continue.



12. Select **Yes, restart the computer now**, and then click **Finish**.

Setup - WinSCP
Completing the WinSCP Setup Wizard
To complete the installation of WinSCP, Setup must restart your computer. Would you like to restart now?
Yes, restart the computer now
No, I will restart the computer later
Help
Finish

Logging on to an Application Server from WinSCP

To log on to the Application Server

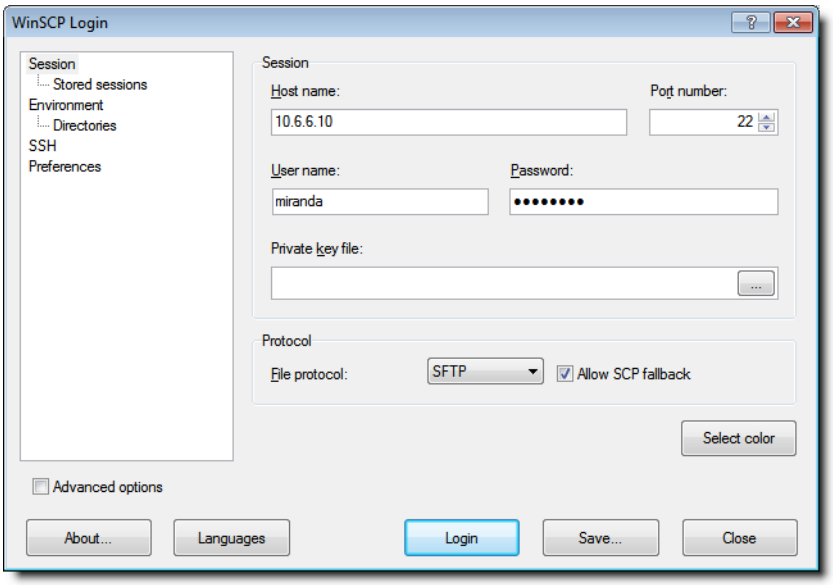
1. Open WinSCP.

   The **WinSCP Login** window appears.

2. Type the Application Server's IP address in the **Host name** box, and specify your user name and password.

Notes

- The default logon accounts are:
  - default IP address: `10.0.3.6`
  - default user name: `miranda`, `root`
  - default password (for both `miranda` and `root`): `icontrol`
- The `miranda` and `root` accounts both have suitable permissions for most applications. However, for some specific purposes such as configuring streaming relays for an Allégro (see "Configuring Allégro Streaming Relays", on page 73), you will need to be logged on as user `root`.

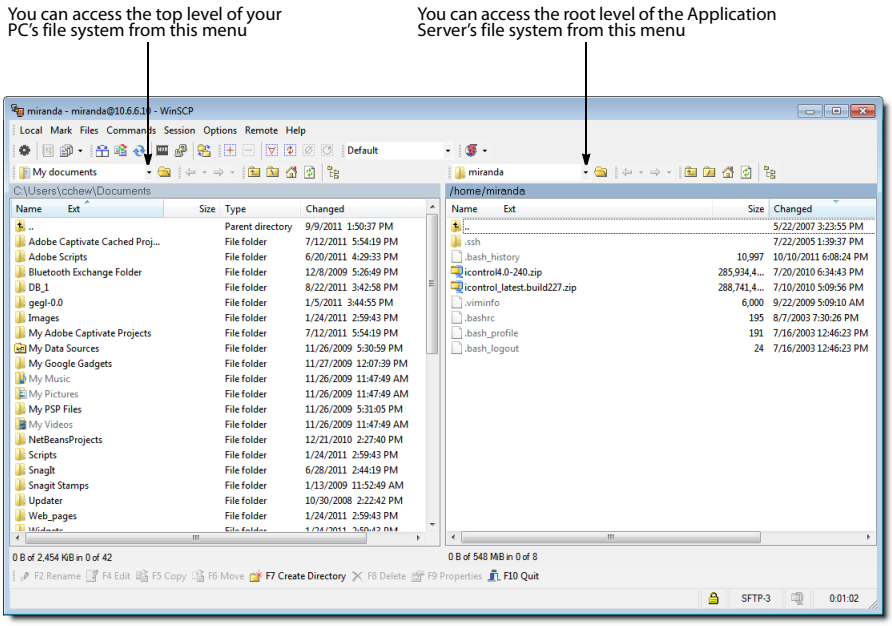


3. Click **Login**.

   A message concerning the server's host key may appear.

4. Click **Yes** to continue.

   The main WinSCP window appears, showing the files on your PC in the left panel, and the files on the Application Server in the right panel.


You can access the top level of your PC's file system from this menu
You can access the root level of the Application Server's file system from this menu
miranda - miranda@10.6.6.10 - WinSCP
Local Mark Files Commands Session Options Remote Help
Default
My documents
miranda
C:\Users\cchew\Documents
/home/miranda
Name Ext Size Type Changed
Name Ext Size Changed
0 B of 2,454 KiB in 0 of 42
0 B of 548 MiB in 0 of 8
F2 Rename F4 Edit F5 Copy F6 Move F7 Create Directory F8 Delete F9 Properties F10 Quit
SFTP-3
0:01:02

Contact Us!

Miranda Technical Support

For technical assistance, please contact the Miranda Technical Support center nearest you:

Americas
Office hours: 9:00 a.m. - 9:00 p.m. (EST)
Telephone: 1-800-224-7882
Fax: +1 514 335 1614
E-mail: support@miranda.com

Asia
Office hours: 9:00 a.m. - 5:00 p.m. (GMT+8)
Telephone: + 852 2539 6987
Fax: + 852 2539 0804
E-mail: asiatech@miranda.com

Europe, Middle-East, Africa, UK
Office hours: 9:00 a.m. - 6:00 p.m. (GMT)
Telephone: + 44 118 952 3444
Fax: + 44 118 952 3401
E-mail: eurotech@miranda.com

China
Telephone: + 86 10 5873 1814
E-mail: asiatech@miranda.com

France
Office hours: 9:00 a.m. - 5:00 p.m. (GMT + 1)
Telephone: + 33 1 55 86 87 88
Fax: + 33 1 55 86 00 29
E-mail: eurotech@miranda.com

EMERGENCY After Hours (Global)
Toll Free: 1-800-224-7882 (US and Canada)
Telephone: +1 514 333 1772

Corporate Head Office

Miranda Technologies Inc.
3499 Douglas-B.-Floreani, St-Laurent, Quebec, Canada H4S 2C6
Telephone: +514 333 1772
Fax: +514 333 9828
Web: http://www.miranda.com